ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ

ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ

Ασφαλής Δρομολόγηση σε Ασύρματα και Κινητά Δίκτυα

Δερμάτης Ζαχαρίας

Επιβλέπων Καθηγητής : Νικόλαος Κολοκοτρώνης

ΠΕΡΙΕΧΟΜΕΝΑ

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή μου κ. Νικόλαο Κολοκοτρώνη κυρίως για την εμπιστοσύνη που μου έδειξε, και την υπομονή που έκανε κατά τη διάρκεια υλοποίησης της πτυχιακής εργασίας

Περίληψη

Η ασφάλεια (security) η οποία αποτελεί ένα από τα σοβαρότερα προβλήματα στα κινητά αδόμητα δίκτυα (Mobile Ad-Hoc networks) είναι δύσκολο να επιτευχθεί, λόγω της ευπάθειας των ασύρματων συνδέσεων, της περιορισμένης φυσικής προστασίας των κόμβων, της δυναμικά μεταβαλλόμενης τοπολογίας τους, της απουσίας μιας αρχής πιστοποίησης (certification authority) αλλά και την έλλειψη ενός κεντρικού σημείου ελέγχου.

Οι διάφορες μελέτες που έχουν γίνει πάνω στην περιοχή των κινητών αδόμητων δικτύων είναι προσανατολισμένες στην πρόταση πρωτοκόλλων τα οποία έχουν ως στόχο την επίλυση μερικών θεμελιωδών προβλημάτων όπως πχ. η δρομολόγηση. Αυτά τα πρωτόκολλα παρόλο που είναι πλήρως αποδεκτά από όλους τους κόμβους ενός τέτοιου δικτύου δεν εξετάζουν το θέμα της ασφάλειας.

Είναι συνεπώς τρωτά σε επιθέσεις και κακόβουλες συμπεριφορές. Ωστόσο πιο πρόσφατες μελέτες εστίασαν σε προβλήματα ασφάλειας και πρότειναν μηχανισμούς προκειμένου να εξασφαλίσουν τόσο τα πρωτόκολλα όσο και τις εφαρμογές. Στόχος της παρούσας εργασίας είναι να ερευνήσουμε και να παρουσιάσουμε αυτές τις μελέτες αλλά και τις προκλήσεις που πηγάζουν μέσα από αυτές. Έτσι λαμβάνοντας όλα τα παραπάνω ως δεδομένα τα ζητήματα ασφαλείας που θα περιληφθούν στην παρούσα εργασία είναι: ζητήματα ασφάλειας δρομολόγησης (routing security issues) για παράδειγμα επιθέσεις στα διάφορα πρωτόκολλα δρομολόγησης, θέματα ασφαλείας κατά την αποστολή δεδομένων(data forwarding), έλεγχος πρόσβασης στο δίκτυο, διαχείριση κλειδιών και ανίχνευση παρείσφρησης, και τέλος οι διάφορες ευπάθειες των χρησιμοποιούμενων πρωτοκόλλων (MAC).

Στα πλαίσια της συγκεκριμένης εργασίας θα εστιάσουμε στα ζητήματα ασφαλείας των κινητών αδόμητων δικτύων και των προκλήσεων που προκύπτουν μέσα από αυτά.

ABSTRACT

The safety (security) which is one of the most serious problems in unstructured mobile networks (Mobile Ad-Hoc networks) is difficult to achieve due to the

vulnerability of wireless links, limited physical protection of nodes, the dynamically changing topology, their absence of a certification authority (certification authority) and the lack of a central control point.

Various studies have been done on the area of mobile unstructured networks are oriented in the proposed protocols that are intended to solve some fundamental problems, such as eg the routing. These protocols even though they are fully accepted by all nodes of such a network not address the issue of security.

It is therefore vulnerable to attacks and malicious behaviors. However more recent studies have focused on security problems and propose mechanisms to ensure both protocols and applications. The aim of this paper is to investigate and present these studies and the challenges arising from these instruments. So taking all the above as data security issues to be included in this work are: security issues routing (routing security issues), for example, attacks on various routing protocols, security issues when sending data (data forwarding), network access control, key management and intrusion detection, and finally the various vulnerabilities used protocols (MAC).

In the context of this work will focus on the security issues of mobile unstructured networks and the challenges that arise within them.

ΚΕΦΑΛΑΙΟ 1^{ο}

1.1Εισαγωγή

Ένα ad hoc δίκτυο είναι μια συλλογή από κόμβους που δεν χρειάζεται να βασίζονται σε μια προκαθορισμένη υποδομή ώστε να κρατήσουν συνδεδεμένο το δίκτυο. Τα Ad hoc δίκτυα μπορούν να διαμορφώνονται, να συγχωνεύονται ή να διαχωρίζονται σε διαφορετικά δίκτυα ακαριαία χωρίς κατ 'ανάγκη να στηρίζονται σε μια σταθερή υποδομή για τη διαχείριση της ενέργειας.[6] Έτσι ένα δίκτυο ad hoc ορίζεται ως "ένα αυτόνομο σύστημα των δρομολογητών που συνδέονται με ασύρματες συνδέσεις, την ένωση των οποίων υποστηρίζει ένας αυθαίρετος γράφος. Οι δρομολογητές είναι ελεύθεροι να κινούνται και να οργώνονται τυχαία και αυθαίρετα. Επομένως η ασύρματη τοπολογία του δικτύου μπορεί να αλλάξει γρήγορα και απρόβλεπτα. Ένα τέτοιο δίκτυο μπορεί να λειτουργεί με ένα αυτόνομο τρόπο ή μπορεί να συνδεθεί με την ευρύτερη λειτουργία του διαδικτύου ως ένα υβριδικό-σταθερό δίκτυο ad hoc. [7]

Οι κόμβοι των Ad Hoc δικτύων είναι συχνά κινητοί το οποίο υποδηλώνει ότι εφαρμόζουν την ασύρματη επικοινωνία για τη διατήρηση της σύνδεσης και η συγκεκριμένη κατηγορία αυτών των δικτύων ονομάζεται κινητά ad hoc δίκτυα ή αλλιώς Mobile Ad Hoc Networks (MANET). Η κινητικότητα δεν είναι ωστόσο η απαίτηση για τους κόμβους σε adhoc δίκτυα και έτσι ενδέχεται να υπάρχουν στατικοί και ενσύρματοι κόμβοι οι οποίοι μπορούν να κάνουν χρήση των υπηρεσιών που προσφέρονται από σταθερές δικτυακές υποδομές. Τα MANETs αποτελούν ένα νέο πρότυπο του ασύρματου δικτύου προσφέροντας απεριόριστη κινητικότητα χωρίς καμία σχετική υποδομή, όπως σταθμό βάσης ή κινητά κέντρα μεταγωγής.

Ένας ορισμός τους παρατίθενται παρακάτω:

Mobile Ad-hoc Network (MANET) είναι ένα αυτο-οργανώσιμο αυτο-σχηματιζόμενο ασύρματο δίκτυο με διαδρομές πολλαπλών τμημάτων (multi-hop), όπου η δομή του δικτύου αλλάζει δυναμικά λόγω της κινητικότητας των κόμβων ή αλλαγών στην τοπολογία.

1.2 Ιστορική Αναδρομή

Η πρώτη γενιά Ad-hoc δικτύων στις αρχές της δεκαετίας του 1970 λεγόταν "packet radio networks" (ραδιοφωνικά δίκτυα πακέτου - PRNET) και βρίσκονταν υπό την αιγίδα του Defense Advanced Research Projects Agency (DARPA). Τα PRNET παρείχαν μέσω ενός κοινού ραδιοφωνικό καναλιού την ανταλλαγή δεδομένων μεταξύ γεωγραφικά χωρισμένων υπολογιστών. Ένα από τα πλεονεκτήματα τους ήταν η κινητικότητα. Ένα πακέτο (PR) θα μπορούσε να λειτουργεί εν κινήσει.

Δεύτερον, δεδομένου ότι δεν υπάρχουν καλώδια για να τρέξει το δίκτυο θα μπορούσε να εγκατασταθεί ή να αναπτυχθεί γρήγορα. Ένα τρίτοπλεονέκτημα είναι η ευκολία στην σχετική ρύθμιση και στην αναδιάταξη. Τα πρωτόκολλα PRNET εκμεταλλεύτηκαν τις ραδιοτηλεοπτικές εκπομπές και τις ιδιότητες των κοινών καναλιών για να επιτρέψουν την επέκταση και την αναπροσαρμογή των δικτύων αυτόματα και δυναμικά. Όταν μια ομάδα πακέτων (PR) εξέρχονταν από την αρχική περιοχή αυτό δεν είχε δυσμενείς επιπτώσεις

για το υπόλοιπο δίκτυο. Τα πακέτα αυτά εγκατέλειπαν το δίκτυο και είχαν την ευελιξία να λειτουργήσουν ως αυτόνομη ομάδα και να επανέλθουν στο αρχικό δίκτυο ή να συμμετάσχουν σε κάποια άλλη ομάδα. Η γενιά των PRNET δικτύων χαρακτηρίστηκε από την πλήρως αυτοματοποιημένη διαχείριση του δικτύου. Ένα PRNET δίκτυο αποτελείται από τα ακόλουθα μέρη :

- Το *υποδίκτυο (subnet) PRNET* με τα ραδιοφωνικά του πακέτα (PR). Το υποδίκτυο PRNET παρείχε τα μέσα της διασύνδεσης της κοινότητας των χρηστών.

- *Μια συλλογή συσκευών (υπολογιστές και τερματικά)* καθένα από τα οποία συνδεόταν με ένα πακέτο PR μέσω ενός υψηλού επιπέδου Data Link Control (HDLC) πρωτοκόλλου για την ανταλλαγή δεδομένων σε πραγματικό χρόνο.[1]

Στη δεκαετία του 1980 τα PRNET δίκτυα εξελίχθηκαν στην **δεύτερη γενιά των ad hoc** δικτύων η οποία είναι γνωστή ως Survivable Adaptive Radio Network (SURAN). Τα SURAN παρείχαν ένα δίκτυο μεταγωγής πακέτου (packet-switched network) της κινητής τηλεφωνίας στο πεδίο της μάχης, σε ένα περιβάλλον δηλαδή χωρίς καμία υπάρχουσα υποδομή. Το SURAN αναπτύχθηκε από την έρευνα για την εξεύρεση λύσεων για την κατασκευή μικρότερων, λιγότερο ακριβών και λιγότερο ευάλωτων σε ηλεκτρονικές επιθέσεις, πακέτων. Τέλος το SURAN εκμεταλλεύτηκε τα πλεονεκτήματα της δικτύωσης των PRNET για το περιβάλλον μάχης ώστε να επιδείξει και έπειτα να αξιολογηθεί ένα ολοκληρωμένο δίκτυο που βασίζεται στην τεχνολογία του. [1]

Η τρίτη γενιά Ad Hoc δικτύων η οποία προέκυψε στην δεκαετία του 1990 την οποία συνεχίζουμε να την χρησιμοποιούμε και σήμερα είναι τα **MANETs.** Οι πιο σημαντικές τεχνολογίες που προέκυψαν εξαιτίας της τεχνολογίας των MANET είναι η δικτύωση *Bluetooth* και τα *AdHoc δίκτυα αισθητήρων*. Το Bluetooth εμφανίστηκε στο προσκήνιο το 1998 περίπου και μας έδωσε τη δυνατότητα υποστήριξης πολλών χρηστών σε οποιοδήποτε περιβάλλον μέσω ενός μικρού δικτύου που είναι γνωστό ως *piconet.* Σε κάθε δεδομένη στιγμή έως και δέκα piconets μπορεί να υπάρχουν στην ίδια περιοχή κάλυψης. Μια συσκευή Bluetooth μπορεί να λειτουργήσει τόσο ως πελάτης (client) όσο και εξυπηρετητής (server) αλλά η ιδιότητα του κάθε εμπλεκόμενου στην σύνδεση θα πρέπει να καθοριστεί πριν τα δεδομένα αρχίσουν να ανταλλάσσονται. Η σύνδεση αυτή ονομάζεται σύζευξη και πρέπει να ζητηθεί πριν την καθιέρωσή της. [1]

Ένα ασύρματο δίκτυο AdHoc αισθητήρων αποτελείται από έναν αριθμό αισθητήρων οι οποίοι κατανέμονται σε μία γεωγραφική περιοχή. Κάθε αισθητήρας έχει δυνατότητα ασύρματης επικοινωνίας και κάποιο επίπεδο νοημοσύνης για την επεξεργασία του σήματος και τη δικτύωση των δεδομένων.

Στο παρόν κεφάλαιο γίνεται πλήρης περιγραφής των Manet δικτύων και στα επόμενα κεφάλαια των επιθέσεων σε αυτά, κατανεμημένων στο πρότυπο OSI. [1]

Ημερομηνία	Γενιά	Εξέλιξη

1972	*1η*	• PRNET (Packet Radio Networks) • ALOHA (Arial Locations of Hazardous Atmospheres) • CSMA (Carrier Sense Medium Access)
1980	*2η*	• SURAN (Survivable Adaptive Radio Networks)
Νωρίτερα από το 1990	*3η*	• GloMo (Global Mobile Information Systems) • NTDR (Near-term Digital Radio) • Σύσταση Ομάδας Εργασίας για τα Manet, 1991.
Μέσα και Αργότερα από το 1990		• JTRS (Joint Tactical Radio System), 1996. • IETF δημοσίευση διάφορων σχεδίων σχετικά με τα πρωτόκολλα δρομολόγησης στα MANET,2000. • IEEE Ίδρυση Εργαστηρίου για τα Manet και την Πληροφορική, 2000.
Μέλλον	*4η*	• Χρήση κινητών adhoc δρομολογητών για την παροχή στους χρήστες σύνδεσης στο Διαδίκτυο . • Κατανεμημένα δίκτυα αισθητήρων. • Δίκτυα αποκατάστασης καταστροφών.

Εικόνα 1. *Ιστορική Ανάπτυξη των Manet . [2]*

1.3 Χαρακτηριστικά των δικτύων Manets

Η αρχή πίσω από την AdHoc δικτύωση είναι η αναμετάδοση με την τεχνική των πολλαπλών αλμάτων (multihops) το οποίο σημαίνει ότι τα μηνύματα διαβιβάζονται από τους άλλους κόμβους εάν ο κόμβος-στόχος δεν είναι άμεσα προσπελάσιμος.

Ένα δίκτυο MANET αποτελείται από κινητές μονάδες (π.χ. ένα δρομολογητή με πολλούς hosts και ασύρματες συσκευές που θα αποκαλούνται κόμβοι) οι οποίες είναι ελεύθερες να μετακινηθούν σε όποια κατεύθυνση επιθυμούν. Αυτοί οι κόμβοι χρησιμοποιώντας τις ασύρματες τεχνολογίες μετάδοσης δεδομένων όπως το *Bluetooth* και το πρωτόκολλο *802.11* μπορούν να βρίσκονται σε αεροπλάνα, πλοία, φορτηγά, αυτοκίνητα, ακόμα και σε ανθρώπους. Ένα δίκτυο MANET λοιπόν, είναι ένα αυτόνομο σύστημα αποτελούμενο από κινητούς κόμβους. Το σύστημα αυτό μπορεί να λειτουργεί απομονωμένο, στο οποίο η απουσία οποιουδήποτε κεντρικού σταθμού βάσεως καθιστά δύσκολη τη διαχείριση του δικτύου και την επικοινωνία με ένα σταθερό δίκτυο. Στον δεύτερο τρόπο λειτουργίας το σύστημα θα λειτουργεί σαν ένα «αποκομμένο δίκτυο» (stub network) που συνδέεται με ένα σταθερό δίκτυο. Τα «αποκομμένα δίκτυα» μεταφέρουν δικτυακή κίνηση που προέρχεται ή κατευθύνεται προς τους εσωτερικούς κόμβους αλλά δεν επιτρέπει η εξωτερική κίνηση να μεταφερθεί μέσω του «αποκομμένου δικτύου».

Οι κόμβοι του δικτύου MANET είναι εξοπλισμένοι με ασύρματους πομπούς και δέκτες χρησιμοποιώντας κεραίες που μπορεί να είναι μη κατευθυντικές (omnidirectional), πολύ-κατευθυντικές (point-to-point), πιθανώς μεταβλητές, ή κάποιος συνδυασμός των

παραπάνω. Σε κάποιο χρονικό σημείο ανάλογα με τη θέση των κόμβων, την εμβέλεια των πομποδεκτών τους, τη μεταδιδόμενη ισχύ τους και τα επίπεδα παρεμβολών, μια ασύρματη σύνδεση στη μορφή ενός τυχαίου AdHoc δικτύου δημιουργείται ανάμεσά τους. Αυτή η AdHoc τοπολογία μπορεί να αλλάξει με την πάροδο του χρόνου καθώς οι κόμβοι μετακινούνται ή αλλάζουν την ισχύ μετάδοσής τους.

Τα βασικά χαρακτηρίστηκα των Manets είναι τα εξής:

- *Μη ύπαρξη καλωδίωσης:* Όπως είναι φυσικό αφού πρόκειται για κινητό - ασύρματο δίκτυο, δεν υπάρχει κάποια μορφή καλωδίωσης όσον αφορά την δικτύωση των κόμβων γεγονός που κάνει πολύ φτηνή και εύκολη την εγκατάσταση του.

- *Δυναμική Τοπολογία:* Η τοπολογία δικτύου σε ένα Manet ασύρματο δίκτυο είναι ιδιαίτερα δυναμική λόγω της κινητικότητας των κόμβων. Μπορεί ο κάθε κόμβος να κινείται μέσα και έξω από την εμβέλεια του άλλου. Η τοπολογία αλλάζει εάν ένα από αυτά τα γεγονότα συμβεί ενώ ο πίνακας δρομολόγησης και ο πίνακας πολύ-εκπομπής πρέπει να αλλάξουν αναλόγως. Αυτό αυξάνει τη δυσκολία στη διαχείριση του δικτύου.

- *Κόμβοι με περιορισμένη κατανάλωση ενέργειας:* Πολλοί, αν όχι όλοι οι κόμβοι σε ένα δίκτυο MANET στηρίζονται σε μπαταρίες. Για το λόγο αυτό η ενέργεια που είναι δυνατόν να καταναλωθεί είναι περιορισμένη, γεγονός που έχει ως αποτέλεσμα η διαχείρισή της να αποτελεί μείζων θέμα για τη βελτιστοποίηση του όλου συστήματος. Προκειμένου να εξοικονομηθεί ενέργεια μερικές συσκευές μπορούν να λειτουργούν με έναν αντίστοιχο τρόπο. Κατά τη διάρκεια αυτής της περιόδου δεν είναι ενδεχομένως προσπελάσιμοι ή δεν επεξεργάζονται την κίνηση που περνά από αυτούς ή μεταπίπτουν στον κανονικό τρόπο λειτουργίας με καθυστέρηση. Από τη μια μεριά, οι περισσότερες ασύρματες συσκευές χρησιμοποιούν τις επικοινωνίες εξάπλωσης φάσματος οι οποίες χρειάζονται τη λήψη και την αποκωδικοποίηση του σήματος. Αυτές είναι ακριβές διαδικασίες που καταναλώνουν πολλή ενέργεια. Αφ' ετέρου, μερικοί σύνθετοι υπολογισμοί είναι επίσης πολύ ακριβοί και καθιστούν δύσκολη την εφαρμογή των συστημάτων δημόσιων κλειδιών στα AdHoc δίκτυα.

- *Περιορισμένο εύρος ζώνης:* Εκτός από την περιορισμένη ηλεκτρική ενέργεια που διατίθεται σε ένα δίκτυο MANET περιορισμοί υπάρχουν και όσον αφορά το εύρος ζώνης του, κάτι που μαζί με την χαμηλή του χωρητικότητα δημιουργούν στις περισσότερες περιπτώσεις προβλήματα συμφόρησης στο δίκτυο. [8]

- *Φθηνοί επεξεργαστές:* Οι περισσότερες κινητές συσκευές έχουν τους φτηνούς και αργούς επεξεργαστές επειδή οι γρήγοροι επεξεργαστές κοστίζουν πολύ περισσότερο. Ως εκ τούτου παίρνει πολύ χρόνο να εκτελεστούν μερικοί σύνθετοι υπολογισμοί.

- *Περιορισμένη ικανότητα αποθήκευσης και άλλων πόρων:* Λόγω των περιορισμών μεγέθους και δαπανών οι περισσότερες κινητές συσκευές είναι εξοπλισμένες με περιορισμένη ικανότητα αποθήκευσης.

- *Κλιμάκωση (Scalability).* Σε κάποια πιθανά δίκτυα MANET όπως στρατιωτικά δίκτυα ή δίκτυα σε αυτοκινητόδρομους ο αριθμός των κόμβων ενδέχεται να είναι σχετικά μεγάλος, μερικές δεκάδες ή ακόμα και εκατοντάδες κόμβοι ανά περιοχή δρομολόγησης (routing area), επομένως απαιτείται η υποστήριξη κλιμάκωσης σε

αυτά τα δίκτυα. Μπορεί η ανάγκη για κλιμάκωση να μην είναι μοναδική για τα MANET αλλά οι μηχανισμοί για την επίτευξή της είναι. [9]

- *Περιορισμένη ασφάλεια σε φυσικό επίπεδο:* Παρόλο που σήμερα χρησιμοποιούνται σε μεγάλο ποσοστό στα κινητά δίκτυα σχεδόν όλες οι μέθοδοι ασφαλείας που υπάρχουν, αυτά παραμένουν ευάλωτα σε φυσικές απειλές, κάτι που δεν παρατηρείται τόσο πολύ στα κλασικά ενσύρματα δίκτυα.

1.4 Εφαρμογές των δικτύων MANET

Τα MANET έχουν πρακτική εφαρμογή σε περιπτώσεις όπου δεν υπάρχει κάποια σταθερή ενσύρματη δικτυακή υποδομή (fixed wired infrastructure). Τέτοιες περιπτώσεις έχουμε όταν δεν είναι οικονομικά, πρακτικά ή γεωγραφικά εφικτό να δημιουργηθεί η απαραίτητη υποδομή ή επειδή οι καταστάσεις δεν επιτρέπουν την εγκατάστασή της, όπως :

- Σε μια συνεδριακή αίθουσα κατά τη διάρκεια συναντήσεων, όταν οι συμμετέχοντες θέλουν να ανταλλάξουν πληροφορίες.

- Σε μια αίθουσα διδασκαλίας κατά τη διάρκεια συζητήσεων με τον καθηγητή ή και κατά τη διάρκεια της διδασκαλίας.

- Σε ένα αεροδρόμιο όπου οι εργαζόμενοι θέλουν να ανταλλάξουν αρχεία.

- Σε μια επείγουσα επιχείρηση διάσωσης, όταν τα μέλη του σωστικού συνεργείου θέλουν να συντονίσουν την προσπάθειά τους. Για παράδειγμα σε περίπτωση όταν κάποιος σεισμός ή πλημμύρα καταστρέψει την ενσύρματη υποδομή των σταθερών δικτύων.

- Σε μάχες κατά τη διάρκεια πολέμου, για τον συντονισμό των στρατιωτών στην άμυνα και την επίθεση.

- Σε δίκτυα που αναφέρονται στη διαμοιρασμένη πρόσβαση στο Internet σε αστικές τοποθεσίες υψηλής πυκνότητας (Neighborhood Area Networks).

Στην παρακάτω εικόνα φαίνονται κατηγοριοποιημένες οι εφαρμογές στα Manet.

Εφαρμογές	Περιγραφή
Τακτικά Δίκτυα	Στρατιωτικές επικοινωνίες στο πεδίο της μάχης.
Δίκτυα Αισθητήρων	Συγκέντρωση ενσωματωμένων συσκευών αισθητήρων που χρησιμοποιούνται για τη συλλογή δεδομένων σε πραγματικό χρόνο και την αυτοματοποίηση των καθημερινών λειτουργιών. Τα δεδομένα συνδέονται άμεσα στο χρόνο και στο χώρο, π.χ. απομακρυσμένοι αισθητήρες για τον καιρό, αισθητήρες για τον εξοπλισμό παραγωγής. Μπορεί να έχουν μεταξύ 1000-100000 κόμβους και κάθε κόμβος να συλλέγει στοιχεία του δείγματος, στη συνέχεια να διαβιβάζει τα δεδομένα στην κεντρική υποδοχή για επεξεργασία χρησιμοποιώντας μικρές ομοιογενείς τιμές.
Υπηρεσίες Έκτακτης Ανάγκης	Εφαρμογές έρευνας και διάσωσης καθώς και αποκατάσταση καταστροφών π.χ. έγκαιρη ανάκτηση και διαβίβαση των δεδομένων των ασθενών (εγγραφές, κατάσταση, διάγνωση) από και προς το νοσοκομείο, αντικατάσταση μιας σταθερής υποδομής σε περίπτωση σεισμών, τυφώνων, πυρκαγιών, κλπ.
Εμπόριο	Ηλεκτρονικό Εμπόριο π.χ. ηλεκτρονικές πληρωμές από οπουδήποτε (δηλαδή απο ένα ταξί), Δυναμικό Επιχειρηματικό Περιβάλλον - πρόσβαση σε αρχεία πελατών που είναι αποθηκευμένα σε μια κεντρική τοποθεσία για την παροχή μιας σταθερής βάσης δεδομένων για όλους σε ένα κινητό γραφείο, μετάδοση ειδήσεων - οδικών συνθηκών - καιρικών συνθηκών.
Σπίτι & Επιχείρηση	Ασύρματη δικτύωση σπιτιού γραφείου (WLAN) π.χ. χρήση PDA για την εκτύπωση σε οποιοδήποτε σημείο, Personal Area Network (PAN), Body Area Network (BAN).
Εκπαίδευση	Δημιουργία εικονικών τάξεων ή αιθουσών συνεδριών.
Διασκέδαση	Πολυχρηστικά παιχνίδια, ρομποτικά κατοικίδια ζώα, εξωτερική πρόσβαση στο Internet.

***Εικόνα 2**. Εφαρμογές των Manets*

1.5 Παράγοντες μιας Επίθεσης

Οι ακόλουθοι είναι οι κύριοι παράγοντες που επηρεάζουν την απόδοση μιας επίθεσης: [5]

- *Υπολογιστική δύναμη* (Computational Power): Αυτό επηρεάζει σαφώς την ικανότητα ενός εισβολέα να υποβιβάσει την ασφάλεια ενός δικτύου. Η εν λόγω δύναμη δεν χρειάζεται για να εντοπιστεί το δίκτυο αλλά για να αναλύσει με μεγάλη ταχύτητα την υποκλέπτουσα (eavesdropped) κυκλοφορία.

- *Ανάπτυξη ικανοτήτων* (Deployment Capability): Ο αριθμός των επιτιθέμενων μπορεί να κυμαίνεται από ένα μόνο κόμβο έως πολλούς «έξυπνους» κόμβους οι οποίοι με συνακόλουθη μεταβολή των δυνατοτήτων τους μπορούν να πραγματοποιήσουν πολύ σοβαρές επιθέσεις.

- *Περιοχή ελέγχου* (Location Control): Η θέση των κόμβων μπορεί να έχει σαφείς επιπτώσεις σε ότι ο αντίπαλος μπορεί να πράξει. Ο αντίπαλος μπορεί να περιορίζεται σε κόμβους στο γεωγραφικό σύνορο ενός δικτύου ή μπορεί να έχει την ικανότητα εκ των υστέρων να δημιουργήσει μια ομάδα «έξυπνων» κακόβουλων κόμβων όπου αυθαίρετα ο βαθμός διεισδυτικότητας στο δίκτυο μπορεί να επιτευχθεί.

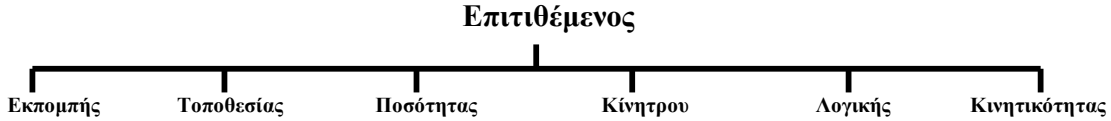
- *Κινητικότητα* (Mobility): Η κινητικότητα φέρνει γενικά αύξηση της ισχύος. Επίσης ένας κινητός κόμβος μπορεί οποιαδήποτε στιγμή να παραμείνει σε στάση. Από την άλλη πλευρά, η κινητικότητα μπορεί να εμποδίσει έναν εισβολέα από το να έχει ως στόχο ένα συγκεκριμένο θύμα. Για παράδειγμα, ένας κόμβος που κινείται ενδέχεται να μην λαμβάνει όλα τα παραποιημένα πακέτα δρομολόγησης που ξεκίνησαν από τον εισβολέα. Συμπερασματικά, ο αντίκτυπος της κινητικότητας για την ανίχνευση, την αποφυγή ή την αταπολέμηση μια επίθεσης είναι ένα σύνθετο θέμα.

- *Ο βαθμός φυσικής πρόσβασης* (Degree of physical access) συμπεριλαμβανομένης της ικανότητας δέσμευσης των κόμβων και της δυνατότητας να προβαίνουν σε φυσική αποδόμηση . [5]

1.6 Είδη επιθέσεων σε δίκτυα Manets.

Μια ποικιλία επιθέσεων είναι δυνατόν να συμβούν σε δίκτυα Manets. Ορισμένες επιθέσεις που ισχύουν για τα ενσύρματα δίκτυα ισχύουν και για ασύρματα δίκτυα και ορισμένες είναι ειδικά για τα MANETs. Αυτές οι επιθέσεις ασφάλειας μπορούν να ταξινομηθούν σύμφωνα με διαφορετικά κριτήρια όπως τον τομέα (domain) των επιτιθέμενων ή τις τεχνικές που χρησιμοποιούνται σε επιθέσεις. Αυτές οι επιθέσεις ασφάλειας στα Manet και σε όλα τα άλλα δίκτυα μπορεί σε γενικές γραμμές να χαρακτηρίζονται από τα εξής κριτήρια: παθητική ή ενεργητική, εσωτερική ή εξωτερική, με βάση το διαφορετικό επίπεδο του προτύπου OSI στο οποίο συμβαίνουν δηλαδή με το πρωτόκολλο επικοινωνίας, με το αν ο επιτιθέμενος είναι ορατός ή κρυφός (stealthy or non-stealthy) και αν συναφείς με την κρυπτογραφία ή όχι.

Οι επιτιθέμενοι μπορούν επίσης να ταξινομηθούν ανάλογα με πολλά κριτήρια όπως της εκπομπής(emission), της τοποθεσίας (location), της ποσότητας (quantity), του κινήτρου (motivation), του ορθολογισμού (rationality) και της κινητικότητας (mobility) τα οποία φαίνονται στην παρακάτω εικόνα. [4]



- Ενεργός
- Παθητικός
- Εσωτερικός
- Εξωτερικός
- Μοναδικός
- Πολλαπλός
- Συνεργαζόμενος Πολλαπλός
- Εμπιστευτικότητα
- Ακεραιότητα
- Ιδιωτικότητα
- Μη Εξουσιοδοτημένη Πρόσβαση
- Ιδιοτέλεια
- Επιβράβευση
- Αφέλεια
- Παραλογισμός
- Ορθολογισμός
- Σταθερός
- Κινητός

Εικόνα 3. *Ταξινόμηση των επιτιθέμενων στα Manets*

Μπορεί επίσης να υπάρχει ένας ή περισσότεροι εισβολείς. Όταν υπάρχουν πολλοί επιτιθέμενοι θα μπορούν να συνεργάζονται μεταξύ τους και έτσι η αντιμετώπιση τους είναι μια δύσκολη περίπτωση. Στο Hu et al. του 2005 δραστηριοποιούνται επιτιθέμενοι οι οποίοι συμβολίζονται ως *Active-nm,* όπου n είναι ο αριθμός των κόμβων που περιέχουν εμπιστευτικές πληροφορίες και m είναι ο συνολικός αριθμός των εμπιστευτικών πληροφοριών, από τους εσωτερικούς και ξένους κόμβους. Προτείνουν, τότε μια ιεραρχία εισβολέα με την αύξηση της δύναμης ως εξής:

- Active-0-1: ο επιτιθέμενος διαθέτει μόνο ένα ξένο κόμβο.
- Active-0-x: ο εισβολέας είναι ιδιοκτήτης x ξένων κόμβων.
- Active-1-x: ο επιτιθέμενος κατέχει x κόμβους και μόνο ένας από αυτούς είναι εσωτερικός.
- Active-y-x: ο επιτιθέμενος διαθέτει x κόμβους και y από αυτούς είναι εσωτερικοί δηλαδή κατέχουν εμπιστευτικές πληροφορίες. [4]

Σημειώνουμε ότι σε αυτή την ιεραρχία όλοι οι κόμβοι αποτελούν ένα απλό εισβολέα. Ως εκ τούτου, υποτίθεται ότι συνεργάζονται μεταξύ τους.

Ένας αντίπαλος εκτελεί *επιθέσεις με κάποια κίνητρα (motivation),* όπως την διάσπαση της εμπιστευτικότητας (confidentiality), της ακεραιότητας (integrity) και της ιδιωτικότητας (privacy). Αυτό μπορεί επίσης να γίνει για να αποκτήσει πρόσβαση σε πόρους με "ευαίσθητες πληροφορίες". Ένας εισβολέας μπορεί επίσης να επιτεθεί για να εμποδίσει τις εργασίες μιας άλλης πλευράς. [4]

Η μη χρησιμοποίηση, η δυσλειτουργία των κόμβων και οι αφελείς (naive) χρήστες μπορούν να γίνουν επίσης απειλές για ένα δίκτυο. Ωστόσο, η μη χρησιμοποίηση των κόμβων δεν είναι ο μόνος λόγος για «παράλογες» επιθέσεις. Ένας εισβολέας μπορεί να επιτεθεί μόνο και μόνο για να επιτεθεί και να «σπάσει» ένα σύστημα ασφαλείας αντιλαμβανόμενος σαν πρόκληση για τον εαυτό του. [4]

Ακόμα οι *ορθολογικοι (rational) εισβολείς* πραγματοποιούν τις επιθέσεις τους για την απόκτηση των κόμβων κάτι που αξίζει περισσότερο από το κόστος της επίθεσης. Επίσης *οι επιτιθέμενοι μπορούν να είναι σταθεροί (fixed) ή κινητοί(mobile). Η* ανίχνευση κινητών επιτιθέμενων όπως και η υπεράσπιση εναντίον τους είναι γενικά πιο δύσκολη από ό, τι απέναντι σε ένα σταθερό αντίπαλο. [4]

1)Ενεργές & Παθητικές Επιθέσεις: Οι επιθέσεις στα Manets μπορούν «χονδρικά» να ταξινομηθούν σε δύο μεγάλες κατηγορίες, δηλαδή στις παθητικές επιθέσεις και στις ενεργές επιθέσεις. Μια παθητική επίθεση λαμβάνει δεδομένα που ανταλλάσσονται στο

δίκτυο χωρίς την διακοπή της λειτουργίας των επικοινωνιών τα οποία μπορούν αργότερα να χρησιμοποιηθούν σε μια ενεργή επίθεση ενώ η ενεργή επίθεση συνεπάγεται διακοπή ενημέρωσης, τροποποίηση ή κατασκευή της πληροφορίας που μεταδίδετε διαταράσσοντας έτσι τη φυσιολογική λειτουργία του δικτύου Manet. Παραδείγματα παθητικών επιθέσεων είναι οι υποκλοπές (eavesdropping), η ανάλυση της κίνησης των δεδομένων (traffic analysis) καθώς η και παρακολούθηση της κυκλοφορίας (monitoring). Παραδείγματα των ενεργών επιθέσεων αποτελούν οι παρεμβολές (jamming), η πλαστοπροσωπία (impersonating), η τροποποίηση (modification), η άρνηση παροχής υπηρεσιών (Denial of Service) και η επανάληψη του μηνύματος (message replay). [10]

Ενεργές Επιθέσεις

Ανακριβής Προώθηση

- *Μη Προώθηση*
- *Αργή Προώθηση*
- *Επανειλημμένη Προώθηση*
- *Προώθηση των Μηνυμάτων στους Επιτιθέμενους για Ανάλυση*

Άρνηση των Υπηρεσιών

- *Ψευδής Πληροφορίες Δρομολόγησης*
- *Νόθευση των Πληροφοριών Δρομολόγησης*
- *Υπερφόρτωση Δικτύου*
- *Έλλειψη μηνυμάτων λάθους, παρόλο που ένα λάθος έχει παρατηρηθεί*

Παθητικές Επιθέσεις

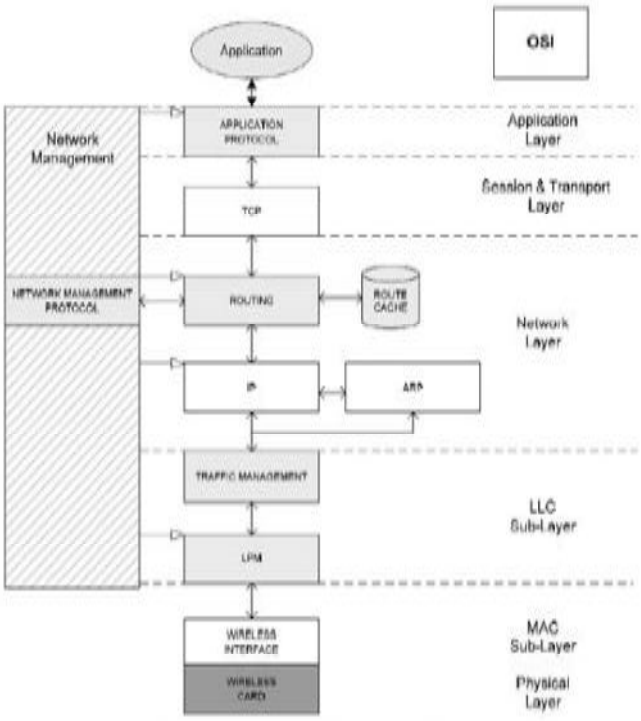
Συγκέντρωση Πληροφοριών (Υποκλοπή)

Εικόνα 4. *Αναλυτική Ταξινόμηση Επιθέσεων(ενεργές-παθητικές) στα Manets*

2)Εσωτερικές & Εξωτερικές Επιθέσεις: Οι επιθέσεις μπορούν επίσης να ταξινομηθούν στις εξωτερικές επιθέσεις και τις εσωτερικές επιθέσεις ανάλογα με τον τομέα επιθέσεων. Οι εξωτερικές επιθέσεις πραγματοποιούνται από τους κόμβους που δεν ανήκουν στην περιοχή του δικτύου και έχουν ως στόχο να προκαλέσουν συμφόρηση, να αναπαράγουν λανθασμένες πληροφορίες δρομολόγησης, ννα εμποδίσουν τις υπηρεσίες να λειτουργήσουν σωστά ή να τις απενεργοποιήσουν κτλ . Οι εσωτερικές επιθέσεις πραγματοποιούνται από κόμβους που στην πραγματικότητα είναι μέρος του δικτύου. Οι εσωτερικές επιθέσεις είναι πιο σοβαρές σε σύγκριση με τις εξωτερικές από την άποψη ότι οι εσωτερικοί - κακόβουλοι κόμβοι γνωρίζουν εμπιστευτικές και απόρρητες πληροφορίες και κατέχουν προνομιακά δικαιώματα πρόσβασης. [10]

Πιο συγκεκριμένα ένας εισβολέας μπορεί να είναι εκ των έσω ή ξένος. Εκ των έσω είναι ένας κόμβος που έχει παραβιαστεί ή παραποιηθεί και αποτελεί μέρος του δικτύου. Ο επιτιθέμενος τότε γνωρίζει όλες τις κρυπτογραφικές πληροφορίες. Ως εκ τούτου, οι Αόρατες (Stealthy) Ενεργές Επιθέσεις μπορούν να οργανωθούν από επιτιθέμενους που κατέχουν εμπιστευτικές πληροφορίες. Εξωτερικές-Ξένες (Outside) επιθέσεις μπορεί να είναι είτε παθητικές ή ενεργές. Με άλλα λόγια ένας εσωτερικός επιτιθέμενος μπορεί να θεωρηθεί ως νομική οντότητα εντός του δικτύου, όπως ένας κόμβος που έχει καταχωρηθεί ή ένας κόμβος που επιτρέπεται να έχει πρόσβαση στο δίκτυο. Ξένος είναι συνήθως ένα κόμβος που δεν είναι ευπρόσδεκτος στο δίκτυο. [4]

3)Επιθέσεις σε διάφορα επίπεδα του προτύπου OSI: Οι επιθέσεις είναι δυνατόν να ταξινομούνται περαιτέρω ανάλογα με το είδος τους και την τεχνικής τους σε πέντε (5) επίπεδα του προτύπου OSI. Το πρότυπο OSI σχεδιάστηκε από τον ISO (International Standard Organization) σύμφωνα με τον όποιο σχεδιάζονται όλα τα δίκτυα μιας και ο OSI είναι ο βασικός οργανισμός τυποποίησης με αναγνώριση σε πολλές χώρες. Η βασική ιδέα του προτύπου είναι ότι τα δεδομένα που διέρχονται από ένα δίκτυο περνάνε από τα επτά (7) διαφορετικά επίπεδα του προτύπου. Τα επίπεδα του προτύπου είναι ιεραρχικά τα εξής: το επίπεδο εφαρμογής, το επίπεδο παρουσίασης, το επίπεδο συνοδού, το επίπεδο μεταφοράς, το επίπεδο δικτύου, το επίπεδο ζεύξης δεδομένων και το φυσικό επίπεδο. Σε κάθε επίπεδο γίνονται ξεχωριστές εργασίες πάνω στα δεδομένα που τα προετοιμάζουν για το επόμενο κατά σειρά επίπεδο. Κάθε επίπεδο δέχεται τις υπηρεσίες του κατώτερου επιπέδου και προσφέρει με την σειρά του τις υπηρεσίες του στο ανώτερο επίπεδο. Η παρακάτω εικόνα παρουσιάζει μια ταξινόμηση των διαφόρων επιθέσεων ασφαλείας σε κάθε επίπεδο του προτύπου OSI. [10] Επίσης ορισμένες επιθέσεις μπορούν να δρομολογηθούν σε πολλά επίπεδα του προτύπου OSI.



Εικόνα 5. *Επικοινωνιακή διαστρωμάτωση των Manet δικτύων στο πρότυπο OSI*

Επίπεδο	Επίθεση	Σκοπός
Εφαρμογής	Κακόβουλου Κώδικα	Μόλυνση των εφαρμογών & και των λειτουργικών συστημάτων
	DoS	Άρνηση παροχής υπηρεσιών
	Snooping	Μη εξουσιοδοτημένη πρόσβαση στα δεδομένα ενός ατόμου
	Άρνησης Συμμόρφωσης	Άρνηση συμμετοχής σε όλη ή μέρος της επικοινωνίας
Μεταφοράς	Άρνησης Υπηρεσιών (DoS)	Άρνηση πρόσβασης σε νόμιμες υπηρεσίες
	Θύελλας ACK μηνυμάτων	Αποσυντονισμός της TCP διαδικασίας
	Session Hijacking (TCP)	Κλοπής ευαίσθητων πληροφοριών
Δικτύου	Επιθέσεις κατά τη φάση ανακάλυψης της διαδρομής (RREQ Attack).	Στοχεύουν στη ανακάλυψη ή στη φάση συντήρησης της δρομολόγησης μη ακολουθώντας τις προδιαγραφές των πρωτοκόλλων δρομολόγησης.
	Rushing	Γρήγορες επιθέσεις εναντίον των on-demand πρωτόκολλων δρομολόγησης
	Αποκάλυψης της Τοποθεσίας	Συγκέντρωση πληροφοριών τοπολογίας
	Καταβόθρας	Συγκέντρωση όλης της κίνησης μιας συγκεκριμένης περιοχής του δικτύου μέσω ενός εκτεθειμένου κόμβου
	Αναπαραγωγής Κόμβου	Προσθήκη ενός κόμβου στο υπάρχον δίκτυο αντιγράφοντας (αναπαράγοντας) το ID ενός υπάρχοντος κόμβου.
	Κατανάλωσης Πόρων	Ανούσια χρήση των Πόρων
	Μαύρης Τρύπας	Πτώση των μηνυμάτων
	Σκουληκότρυπας	Διατάραξη της Δρομολόγησης
Ζεύξης Δεδομένων	Αδυναμία του πεδίου NAV	Αλλοίωση στη συνεχιζόμενη μετάδοση του πλαισίου του επίπεδου ζεύξης δεδομένων μέσω ασύρματων παρεμβολών
	Διαταραχή στο MAC-DCF (Back Off)	Διατάραξη της MAC διαδικασίας
	Διαταραχή στο WEP	Διατάραξη του WEP πρωτοκόλλου
Φυσικό	Υποκλοπή	Απόκτηση ευαίσθητων πληροφοριών
	Φυσική Επίθεση	Φυσική προσέγγιση της κλοπής
	Παρεμβολή	Παρεμπόδιση της επικοινωνίας

***Εικόνα 6**. Επιθέσεις στα Manets στο πρότυπο OSI*

4)Αόρατες (Stealthy) Επιθέσεις: Ορισμένες επιθέσεις ασφαλείας κάνουν χρήση της μυστικότητας σύμφωνα με την οποία οι επιτιθέμενοι προσπαθούν να κρύψουν τις ενέργειές τους είτε από έναν άνθρωπο ο οποίος κάνει παρακολούθηση του συστήματος είτε από ένα σύστημα ανίχνευσης εισβολής (Institution Detection System). Αλλά και άλλες επιθέσεις όπως DoS μπορούν να γίνουν με τον παραπάνω τρόπο. [10]

5)Επιθέσεις που σχετίζονται με την Κρυπτογραφία ή την μη Κρυπτογραφία: Μερικές επιθέσεις σχετίζονται με την μη κρυπτογραφία και άλλες είναι κρυπτογραφικές επιθέσεις. Η παρακάτω εικόνα δείχνει κρυπτογραφικές επιθέσεις και παραδείγματα. [10]

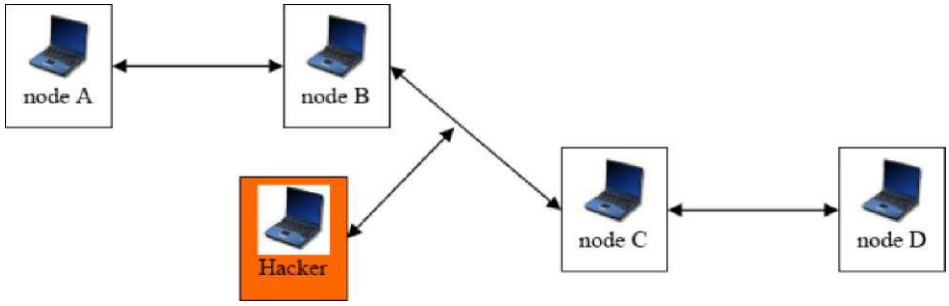
Κρυπτογραφικές Επιθέσεις	Παραδείγματα
Ψευδοτυχαίος αριθμός επιθέσεων	Nonce, Timestamp, Initialization Vector (IV)
Επίθεση Ψηφιακών Υπογραφών	Υπογραφές RSA,EIGamal,DSS
Επίθεση συγκρούσεων Hash	SHA-0,MD4,MD5,HAVAL-128,RIPEMD

***Εικόνα 7.** Επιθέσεις που σχετίζονται με την κρυπτογραφία*

1.7 Πιθανές επιθέσεις στα Manet Πρωτόκολλα δρομολόγησης

Τα πρωτόκολλα δρομολόγησης στα Manet είναι αρκετά ανασφαλή επειδή οι εισβολείς μπορούν εύκολα να λαμβάνουν πληροφορίες σχετικά με την τοπολογία του δικτύου. Πράγματι στα πρωτόκολλα AODV και DSR τα πακέτα εντοπισμού της διαδρομής βρίσκονται σε απλό κείμενο. Έτσι ένας κακόβουλος κόμβος μπορεί να ανακαλύψει τη δομή του δικτύου μόνο με την ανάλυση αυτού του είδους των πακέτων και μπορεί να είναι σε θέση να καθορίσει τον ρόλο του κάθε κόμβου στο δίκτυο. Με όλες αυτές τις πληροφορίες μπορεί να πραγματοποιούνται σοβαρές επιθέσεις με σκοπό να διαταράξουν τη λειτουργία του δικτύου όπως με την απομόνωση σημαντικών κόμβων κλπ. Ας δούμε τις διάφορες δυνατές επιθέσεις με τη χρήση πρώτα της τροποποίησης (modification) στη συνέχεια με τη χρήση της πλαστοπροσωπίας (impersonation) και τέλος τις επιθέσεις οι οποίες χρησιμοποιούν πλαστογραφία (fabrication). [3]

1) Επιθέσεις χρησιμοποιώντας την τροποποίηση (modification): Ένας από τους πιο απλούς τρόπους για ένα κακόβουλο κόμβο να διαταράξει την καλή λειτουργία των Manet δικτύων είναι να εξαγγείλει καλύτερες διαδρομές τους άλλους κόμβους. Αυτό το είδος της επίθεσης βασίζεται στην τροποποίηση της αξίας της καταλληλότητας μιας διαδρομής ή στην αλλοίωση των πεδίων των μηνυμάτων ελέγχου (Denial of Service attacks). [3]

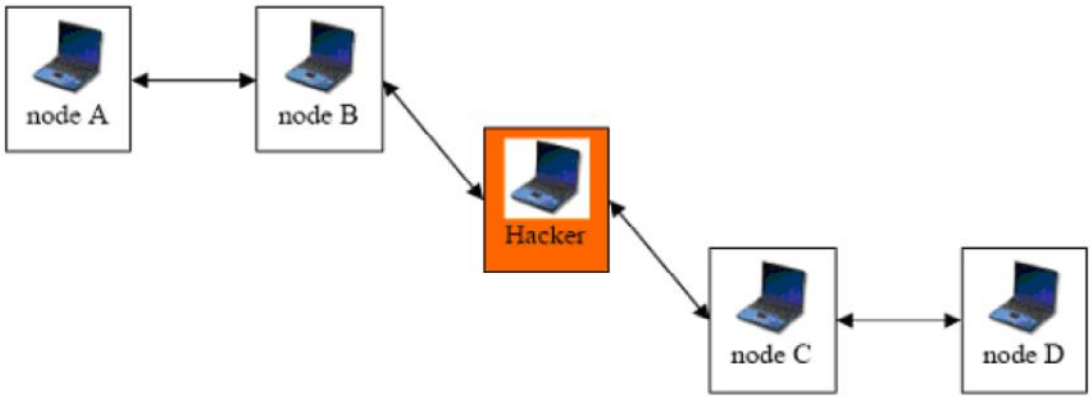


Εικόνα 8. *Επιθέσεις χρησιμοποιώντας την τροποποίηση (modification)*

Για παράδειγμα, στο δίκτυο που φαίνεται στην παραπάνω εικόνα ένας κακόβουλος κόμβος (node) «Hacker» θα μπορούσε να κρατήσει την κίνηση για την πρόσβαση στον κόμβο D μέσω της συνεχούς διαφήμισης στον κόμβο B για μια συντομότερη διαδρομή προς τον κόμβο D από την διαδρομή μέσω του κόμβου C. Οι τρόποι που μπορεί να γίνει αυτό είναι οι εξής:

α) ***Ανακατεύθυνση με την αλλαγή της ακολουθίας του αριθμού της διαδρομής***. Στα Manet δίκτυα όπως και στα ενσύρματα δίκτυα το καλύτερο μονοπάτι για την πρόσβαση σε έναν κόμβο προορισμού καθορίζεται από μια συγκεκριμένη τιμή. Όπως είναι εύκολα αντιληπτό όσο μικρότερη είναι αυτή η τιμή τόσο καλύτερη είναι η διαδρομή. Γι 'αυτό, ένας απλός τρόπος για να επιτεθεί ένας σε ένα δίκτυο είναι να αλλάξει αυτήν την τιμή με έναν μικρότερο αριθμό από το τελευταίο και έτσι θα έχει την "καλύτερη" τιμή.

Στην παρακάτω εικόνα παρατηρούμε επίσης ότι όταν ο κόμβος A θέλει να επικοινωνήσει με τον κόμβο D μεταδίδει ένα μήνυμα ζητώντας από όλους τους κόμβους την καλύτερη διαδρομή για να φτάσει στον κόμβο D. Πιο συγκεκριμένα ο κόμβος B θα λάβει το μήνυμα και προς τα εμπρός. Ο κόμβος C θα απαντήσει ότι έχει μια άμεση διαδρομή προς τον κόμβο D και σε αυτό το μήνυμα απάντησης θα δώσει μια "τιμή" της διαδρομής. Τώρα, αν ο κακόβουλος κόμβος απαντήσει και αυτός στον κόμβο B ότι έχει άμεση διαδρομή προς τον κόμβο D με μικρότερο τιμή από ό, τι ο κόμβος C, ο κόμβος B θα εξετάσει αυτή τη διαδρομή ως την καλύτερη και θα διαγράψει τη διαδρομή με τον κόμβο C. [3]

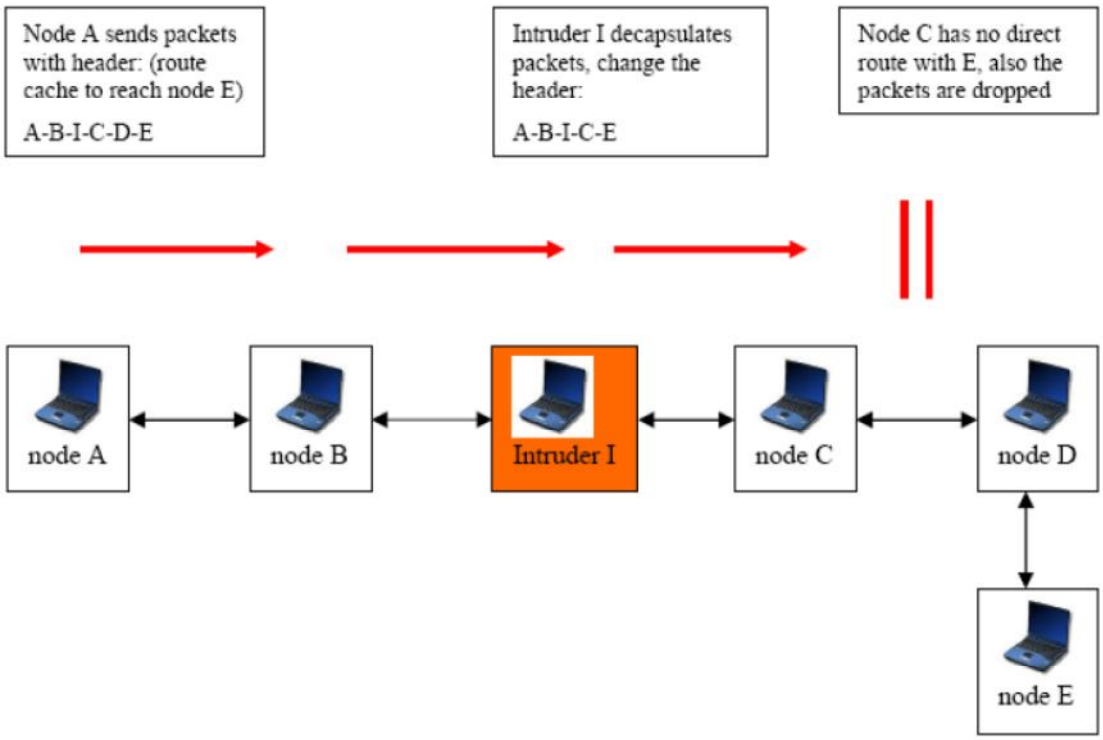


Εικόνα 9. Επίθεση ανακατεύθυνσης με την αλλαγή της ακολουθίας του αριθμού της διαδρομής

β) ***Επίθεση αναπροσανατολισμού με τροποποιημένα άλματα (ειδικά με το πρωτόκολλο AODV).*** Όταν ένας κόμβος δεν μπορεί να αποφασίσει ποια είναι η καλύτερη διαδρομή μπορεί να χρησιμοποιήσει το μέσο αριθμό βημάτων για να αποφασίσει σε ποιο δρόμο βρίσκεται η καλύτερη διαδρομή για να φτάσει σε ένα συγκεκριμένο κόμβο. Αυτή είναι μια περίπτωση του πρωτόκολλου AODV. Στην περίπτωση αυτή, το πρωτόκολλο χρησιμοποιεί την "αξία" των αλμάτων για τον προσδιορισμό της βέλτιστης διαδρομής. Επίσης ένας κακόβουλος κόμβος μπορεί να διαταράξει το δίκτυο πάρα πολύ ανακοινώνοντας μια μικρότερη τιμή αλμάτων για την πρόσβαση ενός κόμβου. Σε γενικές γραμμές, οι κακόβουλοι κόμβοι χρησιμοποιούν την τιμή μηδέν για να είστε σίγουροι ότι έχουν τη μικρότερη τιμή αλμάτων. [3]

*γ)****Denial of Service (DoS) επιθέσεις με τροποποιημένα δρομολόγια από την πηγή***. Η επίθεση DoS είναι γνωστή στην ασφάλεια των υπολογιστών και μπορεί να είναι αποτελεσματική σε AdHoc και κατ επέκταση σε Manet δίκτυα χωρίς ασφαλή πρωτόκολλα δρομολόγησης. Ένας απλός τρόπος για να κατανοήσει κανείς την λειτουργία των DoS επιθέσεων είναι να παρατηρήσει την παρακάτω εικόνα. Στην εικόνα αυτή ένας κακόβουλος κόμβος βρίσκεται στο δίκτυο. Αν ο κόμβος A θέλει να επικοινωνήσει με τον κόμβο E, στέλνει πακέτα δεδομένων σύμφωνα με τα δρομολόγια που υπάρχουν στην μνήμη cache του προς τον κόμβο E συμπεριλαμβανομένου και του κακόβουλου κόμβου. Επίσης, όταν ο κακόβουλος κόμβος θα λάβει τα πακέτα δεδομένων, μπορεί να αλλάξει την κεφαλίδα αυτών των πακέτων ώστε να ματαιωθεί η

διαβίβαση των δεδομένων. Περισσότερα για το συγκριμένο τύπο επιθέσεων θα αναφέρουμε στο αντίστοιχο κεφάλαιο. [3]



Εικόνα 10. *Παράδειγμα DoS Επίθεσης*

2)Επιθέσεις που χρησιμοποιούν πλαστοπροσωπία (impersonation). Οι επιθέσεις αυτές ονομάζονται "spoofing" δεδομένου ότι ο κακόβουλος κόμβος "κρύβει" την IP ή την MAC διεύθυνση του και χρησιμοποιεί μία άλλη. Στα σημερινά Manet πρωτόκολλα δρομολόγησης όπως το AODV και DSR δεν γίνεται έλεγχος ταυτότητας της διεύθυνση IP προέλευσης και έτσι ένας κακόβουλος κόμβος μπορεί να δρομολογήσει πολλές επιθέσεις με τη χρήση της πλαστοπροσωπίας. Για παράδειγμα, ένας κακόβουλος κόμβος μπορεί να δημιουργήσει βρόχους στο δίκτυο και να απομονώσει έναν κόμβο από το υπόλοιπο δίκτυο. Για να γίνει αυτό ο κακόβουλος κόμβος υιοθετεί μια διεύθυνση IP από άλλο κόμβο στο δίκτυο και την χρησιμοποιήσει για να ανακοινώσει μια νέα με μικρότερη τιμή διαδρομή στους άλλους κόμβους. Με αυτόν τον τρόπο μπορεί να τροποποιήσει εύκολα την τοπολογία του δικτύου. [3]

3) Επιθέσεις πλαστογραφίας. Μπορούμε να διακρίνουμε τρία είδη επιθέσεων με τη χρήση της πλαστογραφίας .

- *α) Παραποίηση μηνυμάτων λάθους της διαδρομής*. Η πρώτη επίθεση είναι σύνηθες φαινόμενο στα πρωτόκολλα AODV και DSR επειδή αυτά τα δύο πρωτόκολλα χρησιμοποιούν τη συντήρηση των δρομολογίων για να ανακτήσουν την καλή πορεία όταν πρέπει να κινηθούν σε κάποιες κόμβους. Η αδυναμία αυτής της αρχιτεκτονικής είναι ότι όταν κινείται ένας κόμβος, ο πλησιέστερος κόμβος του στέλνει μήνυμα

λάθους στους άλλους για να τους ενημερώσει ότι η διαδρομή δεν είναι πλέον διαθέσιμη. Αν ένας κακόβουλος κόμβος υποκλέψει την ταυτότητα ενός άλλου κόμβου χρησιμοποιώντας πλαστογράφηση θα αποστείλει μηνύματα λάθους στους άλλους κόμβους και έτσι οι άλλοι κόμβοι θα ενημερώσουν τους πίνακες δρομολόγησης τους με αυτές τις πληροφορίες. Επίσης, ο κακόβουλος κόμβος μπορεί να απομονώσει κάθε κόμβο αρκετά εύκολα.

- *β*) Επιθέσεις μόλυνσης-δηλητηρίασης της κρυφής (cache) μνήμης. Αυτή είναι μια παθητική επίθεση που μπορεί να προκύψει στο DSR πρωτόκολλο κυρίως λόγω της ετερόκλητης λειτουργία του πίνακα δρομολόγησης του εν λόγο πρωτοκόλλου. Αυτό συμβαίνει όταν οι πληροφορίες που είναι αποθηκευμένες στον πίνακα δρομολόγησης σε δρομολογητές διαγράφονται ή αλλοιώνονται με ψευδή στοιχεία. Πράγματι, εκτός από την εκμάθηση δρομολόγιων από τις επικεφαλίδες των πακέτων τις οποίες ένας κόμβος επεξεργάζεται κατά μήκος μιας διαδρομής, στο πρωτόκολλο DSR οι διαδρομές μπορούν επίσης να γνωστοποιηθούν από ετερόκλητα πακέτα που λήφθηκαν από τους κόμβους. Ένας κόμβος ακούει κάθε πακέτο και μπορεί να προσθέσει πληροφορίες δρομολόγησης που περιέχονται στο πακέτο της επικεφαλίδας από την κρυφή μνήμη του, έστω και αν ο κόμβος δεν βρίσκεται στο μονοπάτι από την πηγή προς τον προορισμό.

Η ευπάθεια του συστήματος αυτού είναι ότι ένας εισβολέας θα μπορούσε να εκμεταλλευτεί εύκολα αυτή τη μέθοδο εκμάθησης των διαδρομών και να τις αλλοιώσει. Για παράδειγμα ο κακόβουλος κόμβος έχει μόλις μεταδώσει ένα μήνυμα με πλαστή διεύθυνση IP στους άλλους κόμβους. Όταν οι κόμβοι λάβουν αυτό το μήνυμα θα προσθέσουν τη νέα διαδρομή στην κρυφή μνήμη τους και επίσης θα επικοινωνήσουν τώρα με αυτή τη διαδρομή για να καταλήξουν στον κακόβουλο κόμβο στην πραγματικότητα και όχι με τον κόμβο που είχε την ορθή διεύθυνση IP . [3]

Άλλες επιθέσεις με τη χρήση της πλαστογραφίας (fabrication) είναι οι ακόλουθες:

- *Επίθεση Επανάληψης (Replay Attack):* ένας εισβολέας στέλνει παλιές διαφημίσεις σε έναν κόμβο με αποτέλεσμα να ενημερώσει τον πίνακα δρομολόγησης με ψευδής πλέον πληροφορίες.

- *Επίθεση Μαύρης Τρύπας (Black Hole):* ένας εισβολέας διαφημίζει μια διαδρομή προς όλους τους προορισμούς ώστε να προκαλέσει όλους τους κόμβους να δρομολογήσουν όλα τα πακέτα τους προς αυτή την κατεύθυνση. [3]

4)Επιθέσεις δρομολόγησης υπερχείλισης πίνακα. Αν ένα ad-hoc δίκτυο χρησιμοποιεί ένα προληπτικό (proactive) πρωτόκολλο, αυτό σημαίνει όπως έχουμε προηγούμενα πει ότι ο αλγόριθμος του πρωτοκόλλου θα προσπαθήσει να αναζητήσει πληροφορίες δρομολόγησης ακόμη και όταν αυτό δεν είναι απαραίτητο. Πρόκειται για μια ευπάθεια που χρησιμοποιείται από αυτήν την επίθεση διότι ο εισβολέας προσπαθεί να δημιουργήσει διαδρομή η οποία δεν υφίστανται. Αν δημιουργηθούν τώρα αρκετά δρομολόγια, αυτά δεν θα μπορούν να εκτελεστούν λόγου της ανικανότητας διαχείρισης

του πρωτοκόλλου εξαιτίας της υπερχείλισης του πίνακα δρομολόγησης τους (cache memory). [3]

Στο παρόν κεφάλαιο έγινε μια απλή γενική αναφορά των επιθέσεων τις οποίες θα δούμε αναλυτικά στα επόμενα κεφάλαια.

ΚΕΦΑΛΑΙΟ 2^{Ο}

2.1 Δρομολόγηση σε Ασύρματα Κινητά Δίκτυα

1) Ορισμός του Προβλήματος. Είναι σαφές ότι η δρομολόγηση σε ένα Mobile Ad-Hoc δίκτυο (MANET) είναι εγγενώς διαφορετική από την δρομολόγηση στα κλασικά ενσύρματα δίκτυα. Η δρομολόγηση σε ένα τέτοιο δίκτυο εξαρτάται από πολλούς παράγοντες συμπεριλαμβανομένης της τοπολογίας των κόμβων, της επιλογής των διαδρομών, της κινητικότητας των κόμβων του δικτύου, την πρωτοβουλίας έκδοσης ενός νέου αιτήματος δρομολόγησης και άλλων χαρακτηριστικών που θα μπορούσαν να εξυπηρετήσουν στην εύρεσης των βέλτιστων διαδρομών γρήγορα και αποτελεσματικά. Η μικρή διαθεσιμότητα πόρων στα ad-hoc ασύρματα δίκτυα απαιτεί αποδοτική χρησιμοποίηση τους και ως εκ τούτου επιβάλει την βέλτιστη δρομολόγηση των δεδομένων. Επίσης, η ιδιαίτερα δυναμική φύση των ad-hoc δικτύων επιβάλλει την ύπαρξη αυστηρών περιορισμών στη δρομολόγηση των πρωτοκόλλων που σχεδιάζονται συγκεκριμένα για αυτά, επηρεάζοντας κατά συνέπεια τις κατευθύνσεις στην μελέτη και έρευνα που συντελείτε γύρω από αυτά τα πρωτόκολλα. Μια από τις σημαντικότερες προκλήσεις στο σχεδιασμό ενός πρωτοκόλλου δρομολόγησης για ένα ad-hoc δίκτυο είναι το γεγονός ότι, από τη μια πλευρά, κάθε κόμβος του δικτύου πρέπει να κατέχει πληροφορίες τουλάχιστον για τις ενεργές συνδέσεις με τους γείτονές του για τον καθορισμό μιας διαδρομής και αφ' ετέρου η τοπολογία των δικτύων αυτών μπορεί να αλλάξει αρκετά συχνά με αποτέλεσμα να αλλάζει και τοσύνολο των γειτόνων του κάθε κόμβου. Επιπλέον, καθώς ο αριθμός των κόμβων του δικτύου μπορεί να είναι αρκετά μεγάλος, η εύρεση μιας διαδρομής προς κάποιο προορισμό απαιτεί επίσης τη συχνή ανταλλαγή πληροφοριών δρομολόγησης μεταξύ των κόμβων. Κατά συνέπεια, ο όγκος των νέων πληροφοριών δρομολόγησης είναι αρκετά μεγάλος και αυξάνεται όταν στο δίκτυο υπάρχουν κόμβοι υψηλής κινητικότητας. Οι κόμβοι αυτοί μπορούν να προκαλέσουν μεγάλες καθυστερήσεις και συμφόρηση στο ασύρματο κανάλι κάνοντας αδύνατη ή πολύ δύσκολη την μετάδοση πραγματικών δεδομένων.

2) Το πρόβλημα της Δρομολόγησης στα Ασύρματα ad-hoc Δίκτυα:Το πρόβλημα της δρομολόγησης σε ένα ασύρματο ad-hoc τηλεπικοινωνιακό δίκτυο, το οποίο αποτελείται από κινητούς κόμβους, ορίζεται ως η διαδικασία εύρεσης μιας διαδρομής από έναν κόμβο του δικτύου προς ένα άλλο κόμβο του ίδιου δικτύου με σκοπό την μεταφορά δεδομένων. Ως διαδρομή σε ένα ασύρματο ad-hoc δίκτυο ορίζουμε την ακολουθία των κόμβων μέσω των οποίων θα διαβιβαστούν τα πακέτα δεδομένων στον προορισμό τους. Υποθέτουμε ότι οι κόμβοι, στο δίκτυο αυτό, δεν μπορούν να μεταβιβάσουν απευθείας τα δεδομένα ο ένας στον άλλο, λόγω της περιορισμένης εμβέλειας του ασύρματου πομπού

και γι' αυτό χρησιμοποιούνται ενδιάμεσοι κόμβοι για να μπορέσουν να μεταδοθούν τα δεδομένα στον προορισμό τους. Οι κόμβοι σε ένα ασύρματο ad-hoc δίκτυο στις περισσότερες περιπτώσεις μπορούν και κινούνται, με αποτέλεσμα η θέση τους στο δίκτυο να αλλάζει συνεχώς. Καθώς αλλάζει η θέση τους, αλλάζει και η κατάσταση του δικτύου, άλλες συνδέσεις γίνονται ενεργές, άλλες ανενεργές, νέοι κόμβοι εισέρχονται και προσθέτονται στο δίκτυο, ενώ άλλοι απομακρύνονται και αποβάλλονται. Το γεγονός αυτό επιβάλει οι κόμβοι του δικτύου άλλες φορές να παίζουν το ρόλο τερματικών κόμβων, που είναι είτε οι κόμβοι προέλευσης είτε οι κόμβοι του προορισμού των πακέτων, που ταξιδεύουν στο δίκτυο και άλλες το ρόλο των δρομολογητών ή των μεταγωγέων, που φροντίζουν να προωθήσουν πακέτα, που δεν προορίζονται γι' αυτούς στους κόμβους προορισμού. Για το λόγο αυτό, σε ένα ασύρματο ad-hoc δίκτυο είναι απαραίτητο ένα πρωτόκολλο δρομολόγησης, για να διατηρηθούν οι βασικές λειτουργίες του δικτύου, τις οποίες τώρα έχουν επιφορτιστεί οι κόμβοι.

3) Δρομολόγηση στο Επίπεδο των Συνδέσεων: Στη δρομολόγηση στο επίπεδο συνδέσεων κάθε κόμβος διατηρεί μια άποψη της τοπολογίας του δικτύου με ένα βάρος για κάθε σύνδεση. Κάθε κόμβος μεταδίδει σε όλους του υπόλοιπους κόμβους περιοδικά τις πληροφορίες δρομολόγησης που κατέχει, τις οποίες λαμβάνουν οι υπόλοιποι κόμβοι του δικτύου και ενημερώνουν του πίνακες με τις δικές τους πληροφορίες δρομολόγησης. Στη συνέχεια εφαρμόζοντας έναν αλγόριθμό εύρεσης της συντομότερης διαδρομής επιλέγουν τον επόμενο κόμβο για κάθε ξεχωριστό προορισμό. Ασυνεπείς απόψεις της τοπολογίας του δικτύου μπορούν να οδηγήσουν στο σχηματισμό βρόχων στις διαδρομές, πράγμα που επηρεάζει την απόδοση του αλγόριθμου δρομολόγησης και σκοπός είναι ο εντοπισμός και η απαλοιφή αυτών.

4) Δρομολόγηση με την Χρήση του Διανύσματος της Απόστασης: Κάθε κόμβος κοιτάει μόνο το κόστος των εξερχόμενων συνδέσεών του και αντί της μετάδοσης αυτών των πληροφοριών σε όλους τους κόμβους, μεταδίδει περιοδικά σε κάθε ένα από τους γείτονές του την δικιά του εκτίμηση της πιο σύντομης διαδρομής προς κάθε άλλο κόμβο στο δίκτυο. Οι κόμβοι που λαμβάνουν την πληροφορία αυτή την χρησιμοποιούν για να υπολογίσουν εκ νέου τις διαδρομές προς όλους τους κόμβους του δικτύου, χρησιμοποιώντας ενός αλγορίθμου εύρεσης των συντομότερων μονοπατιών.

5) Δρομολόγηση Πηγής: Η δρομολόγηση πηγής περιγράφει ότι κάθε πακέτο έχει ενσωματωμένο το πλήρες μονοπάτι προς τον κόμβο προορισμού. Ο ενδιαφερόμενος κόμβος συλλέγει όλες τις δυνατές επιλογές διαδρομών και επιλέγει την καλύτερη, σύμφωνα με ένα μέτρο σύγκρισης. Το πλεονέκτημα της μεθόδου αυτής είναι ότι είναι πολύ εύκολο να αποφευχθούν οι κυκλικοί βρόχοι στις διαδρομές δρομολόγησης, αφού ο κόμβος που επιλέγει μια διαδρομή μπορεί να εξασφαλίσει ότι δεν περιέχει βρόγχους. Το μειονέκτημα είναι ότι για κάθε πακέτο απαιτείται μία μικρή αρχική καθυστέρηση για την εύρεση μιας διαδρομής.

6) Τεχνική Πλημμύρας: Πολλά πρωτοκόλλα δρομολόγησης για να μεταδώσουν πληροφορίες δρομολόγησης, τις εκπέμπουν από τον κόμβο προέλευσης προς όλους τους άλλους κόμβους του δικτύου με την τεχνική της πλημμύρας. Η τεχνική αυτή είναι μια ευρέως χρησιμοποιημένη μορφή ασύρματης μετάδοσης και λειτουργεί ως εξής. Ο κόμβος προέλευσης στέλνει τις πληροφορίες του στους γείτονές του (στην ασύρματη

περίπτωση, αυτό σημαίνει, σε όλους τους κόμβους που είναι μέσα στη εμβέλεια του πομπού). Οι γείτονες αναμεταδίδουν στους γείτονές τους τις πληροφορίες που λαμβάνουν. Η διαδικασία αυτή συνεχίζεται έως ότου οι πληροφορίες δρομολόγησης παραληφθούν από όλους τους κόμβους του δικτύου. Ένας κόμβος αναμεταδίδει κάθε πακέτο μόνο μια φορά. Αν λάβει ξανά πακέτο που έχει ήδη προωθήσει απλά το αγνοεί και για να το εξασφαλίσει αυτό χρησιμοποιεί έναν αριθμό ο οποίος αυξάνεται για κάθε νέο πακέτο που ο κόμβος στέλνει.

7) Proactive versus Reactive Πρωτόκολλα Δρομολόγησης: Στα πρωτόκολλα δρομολόγησης βασική λειτουργία είναι η διαδικασία εύρεσης των διαδρομών ανάμεσα στους κόμβους του δικτύου. Ένα από τα πιο ενδιαφέροντα ερευνητικά θέματα, ιδιαίτερα τα τελευταία χρόνια, είναι το εάν οι κόμβοι σε ένα ad- hoc δίκτυο θα πρέπει να κρατούν στοιχεία για κάθε δυνατή διαδρομή ανάμεσα σε δύο οποιοδήποτε κόμβους του δικτύου ή θα πρέπει να κρατούν στοιχεία μόνο για τις διαδρομές εκείνες που είναι άμεσου ή μεγάλου ενδιαφέροντος. Στην πράξη αυτό που συμβαίνει είναι ότι οι κόμβοι του δικτύου δεν χρειάζονται κάποια διαδρομή προς ένα άλλο κόμβο παρά μόνο στην περίπτωση που χρειαστούν να στείλουν δεδομένα προς αυτόν, είτε αυτός είναι ο κόμβος προορισμού των δεδομένων, είτε είναι ένας ενδιάμεσος κόμβος που πρέπει να περάσουν τα δεδομένα για να φτάσουν στον τελικό προορισμό τους. Η έρευνα και η ανάλυση που γίνεται, πάνω σε διάφορα σενάρια και πρωτόκολλα έχει ως στόχο να αποδείξει ποια από τις δύο απόψεις είναι η πιο αποδοτική και γιατί.

Τα πρωτόκολλα τα οποία κρατούν στοιχεία για όλες τις πιθανές διαδρομές που μπορεί να χρειαστούν οι κόμβοι σε ένα δίκτυο έχουν το πλεονέκτημα ότι όταν ζητηθεί μία συγκεκριμένη διαδρομή, από οποιοδήποτε σημείο του δικτύου σε οποιοδήποτε άλλο, αυτή θα υπάρχει και θα προωθηθεί προς χρήση χωρίς καθυστέρηση. Με άλλα λόγια όποια διαδρομή και αν επιθυμούμε να ζητήσουμε προς χρήση, αν υπάρχει, θα μπορούμε να την έχουμε στη διάθεση μας χωρίς να περιμένουμε, επειδή η διαδικασία αναζήτησης έχει ήδη ολοκληρωθεί και τα αποτελέσματα βρίσκονται έτοιμα προς χρήση. Τέτοια πρωτόκολλα ονομάζονται proactive και το βασικό χαρακτηριστικό είναι ότι περιοδικά αναζητούν όλες τις πιθανές διαδρομές προς κάθε κόμβο του δικτύου, για να μπορούν να τις χρησιμοποιήσουν όποια στιγμή τις χρειαστούν.

Από την άλλη μεριά έχουμε τα πρωτόκολλα τα οποία ενεργοποιούν την διαδικασία εύρεσης ενός μονοπατιού (διαδρομής) από ένα κόμβο σε ένα άλλο, μόνο όταν εκδοθεί από τον ενδιαφερόμενο κόμβο ανάλογο αίτημα. Τα πρωτόκολλα αυτά είναι φυσικό να κάνουν σαφώς μικρότερη χρήση του εύρους καναλιού σε σχέση με τα προηγούμενα πρωτόκολλα για την εύρεση των ζητούμενων διαδρομών. Έχουν όμως το σημαντικό μειονέκτημα της αρχικής καθυστέρησης κάθε φορά που ζητείται μία διαδρομή, αφού πριν προωθηθεί στον αιτούντα κόμβο πρέπει να ενεργοποιηθεί η διαδικασία εύρεσης και μετά να τον εξυπηρετήσουν.[3]

8) Ομάδα Εργασίας MANET: Ο σκοπός αυτής της ομάδας εργασίας είναι η τυποποίηση πρωτοκόλλων δρομολόγησης IP, κατάλληλα για την εφαρμογή τους σε ασύρματα στατικά και δυναμικά τηλεπικοινωνιακά δίκτυα επικοινωνιών. Η θεμελιώδης σχεδιαστική αρχή των πρωτοκόλλων αυτών είναι τα ιδιαίτερα χαρακτηριστικά που έχουν οι ασύρματες συνδέσεις σε ένα δίκτυο και το πώς αυτά μπορούν να επηρεάσουν ένα

πρωτόκολλο δρομολόγησης. Η δρομολόγηση σε ένα δυναμικό ασύρματο δίκτυο επηρεάζεται σε πολύ μεγάλο βαθμό από παράγοντες όπως, οι σχετικές θέσεις των κόμβων στο δίκτυο, η κίνηση των κόμβων, η εμβέλεια των ασύρματων πομποδεκτών, τα φυσικά εμπόδια ή άλλες πηγές παρεμβολής που μπορεί να επηρεάζουν την μετάδοση. Τα χαρακτηριστικά αυτά και άλλα τα οποία δεν αναφέρουμε, έχουν σαν αποτέλεσμα η δρομολόγηση να πρέπει να εκτελείται δυναμικά κάτω από διαφορετικές συνθήκες κάθε φορά. Το ζητούμενο λοιπόν και ο στόχος της συγκεκριμένης ομάδας εργασίας είναι η έρευνα και η μελέτη υποψήφιων πρωτοκόλλων δρομολόγησης, τα οποία θα μπορούν να ικανοποιούν τις ιδιαίτερες ανάγκες που παρουσιάζουν τα ασύρματα δίκτυα.

Στο παρελθόν αυτή η ομάδα εργασίας έχει εστιάσει την έρευνα της σε μια ευρεία σειρά από προβλήματα και ζητήματα απόδοσης των σχετικών υποψηφίων πρωτοκόλλων. Πλέον όμως ο σκοπός της είναι η συγκέντρωση και η προώθησης των προδιαγραφών διάφορων πρωτοκόλλων δρομολόγησης σε μορφή RFC (Request For Comments). Μερικά από τα πρωτόκολλα αυτά είναι ο AODV, ο DSR, ο OLSR και το TBRPF. Τα πρωτόκολλα που αναφέραμε είναι αυτά τα οποία παρέμειναν υποψήφια για την έκδοση του τελικού προτύπου, μέσα από μια πλειάδα προτάσεων και υποψηφιοτήτων. Μπορούμε να πούμε ότι είναι τα περισσότερο ώριμα πρωτόκολλα, όσο αφορά την κατανόηση και εφαρμογή των ιδιαίτερων χαρακτηριστικών των MANETs, κάτι που βρίσκουμε σε κάθε ένα από αυτά τα πρωτόκολλα. Αν και αυτά παρέχουν ένα βασικό σύνολο πρωτοκόλλων που καλύπτουν τις απαιτήσεις των MANETs, απαιτείται περισσότερη εμπειρία και πειραματισμός για την απόκτηση μιας καλύτερης άποψης για την συνολική τους απόδοση. Τελικός σκοπός της ομάδας εργασίας αυτής είναι λοιπόν να συντονίσει όλη αυτή την συζήτηση και έρευνα και να βοηθήσει στην καλύτερη και γρηγορότερη αξιοποίηση των γνώσεων και των συμπερασμάτων που εξάγονται από την έρευνα που γίνεται από πολλές ομάδες πάνω στην δρομολόγηση στα Mobile Ad-hoc Networks.

Πάνω σε αυτή τη βάση η ομάδα εργασίας μετά την ολοκλήρωση της έρευνας και της εξαγωγής των συμπερασμάτων και των αποτελεσμάτων θα προσπαθήσει να σχεδιάσει, να αναπτύξει και να καθιερώσει ένα σύνολο κοινών χαρακτηριστικών δρομολόγησης, που πρέπει να έχει κάθε αλγόριθμος δρομολόγησης σε ένα ad-hoc mobile δίκτυο και θα το καταθέσει στον διεθνή οργανισμό Internet Standards. Οι γνώσεις που θα αποκτηθούν από την έρευνα στα υπάρχοντα πρωτόκολλα θα χρησιμοποιηθούν σαν βάση για την δημιουργία των σχεδιαστικών αρχών, για να προκύψει ένα νέο πρωτόκολλο δρομολόγησης, που θα είναι καθολικά αποδεκτό και αποδοτικό σε κάθε περίπτωση.

Ως τμήμα αυτής της προσπάθειας η ομάδα εργασίας θα εξετάσει τις πτυχές της ασφάλειας και του ελέγχου συμφόρησης στα πρωτόκολλα δρομολόγησης.

2.2 Περιγραφή Πρωτοκόλλων Δρομολόγησης των MANET's.

1)Proactive και Reactive Πρωτόκολλα Δρομολόγησης: Τα ad-hoc πρωτόκολλα δρομολόγησης μπορούν να ταξινομηθούν ως Proactive και Reactive. Τα πρώτα εξουσιοδοτούν τους κόμβους σε ένα ad-hoc κινητό δίκτυο να ανακαλύπτουν και να

γνωρίζουν τις διαδρομές προς όλους τους πιθανούς προορισμούς του δικτύου έτσι ώστε, όταν πρέπει να διαβιβαστεί ένα πακέτο, να είναι ήδη γνωστή η διαδρομή που αυτό πρέπει να ακολουθήσει. Τα πρωτόκολλα της δεύτερης κατηγορίας υιοθετούν μια διαφορετική προσέγγιση με την οποία οι κόμβοι ανακαλύπτουν μόνο τις διαδρομές προς αυτούς τους προορισμούς, για τους οποίους γίνεται σχετική αίτηση εύρεσης μιας διαδρομής. Ένας κόμβος δεν χρειάζεται να γνωρίζει μια διαδρομή προς ένα προορισμό, παρά μόνο όταν πακέτα δεδομένων τα οποία πρέπει να προωθήσει, έχουν σαν τελικό προορισμό τους τον κόμβο αυτό. Τα proactive πρωτόκολλα έχουν το πλεονέκτημα ότι ένας κόμβος υπόκειται στην ελάχιστη καθυστέρηση για την απόκτηση μιας διαδρομής, αφού αυτή αν υπάρχει θα είναι διαθέσιμη στους πίνακες δρομολόγησης του συγκεκριμένου κόμβου. Εντούτοις τα πρωτόκολλα αυτά δεν είναι αποδοτικά σε όλες τις περιπτώσεις και σενάρια χρήσης, δεδομένου ότι χρησιμοποιούν ένα ουσιαστικό μέρος των πόρων του δικτύου για την διατήρηση και ανανέωση των πληροφοριών δρομολόγησης που γνωρίζουν οι κόμβοι. Για να αντιμετωπίσουν ακριβώς αυτό το μειονέκτημα, τα re-active πρωτόκολλα υιοθετούν την προσέγγιση της εύρεσης μιας διαδρομής για έναν προορισμό μόνο όταν αυτό απαιτείται. Τα re-active πρωτόκολλα καταναλώνουν πολύ λιγότερους πόρους σε σχέση με τα προηγούμενα, αλλά η αρχική καθυστέρηση εύρεσης μιας διαδρομής μπορεί να είναι σημαντικά μεγάλη και μπορεί να είναι, αν όχι μεγαλύτερη, συγκρίσιμη με τον χρόνο που απαιτείται για την μεταφορά των πραγματικών δεδομένων ανάμεσα σε δύο κόμβους. Εν συντομία, μπορούμε να καταλήξουμε στο συμπέρασμα ότι κανένα πρωτόκολλο δεν είναι υλοποιημένο να λειτουργεί το ίδιο αποδοτικά και αποτελεσματικά σε όλα τα πιθανά δικτυακά περιβάλλοντα και γι' αυτό έχουν γίνει προτάσεις που χρησιμοποιούν υβριδικές προσεγγίσεις για την αντιμετώπιση αυτού του προβλήματος.

2.3 Proactive Πρωτόκολλα Δρομολόγησης (Table Driven)

Σε αυτό το τμήμα εξετάζουμε μερικά από τα σημαντικότερα proactive πρωτόκολλα δρομολόγησης.

1) Destination Sequenced Distance Vector Routing Protocol: Το (DSDV) είναι ένα δυναμικό πρωτόκολλο, που χρησιμοποιεί διανυσματικές αποστάσεις, βάση των συνδέσεων από τις οποίες αποτελείται κάθε διαδρομή, για την δρομολόγηση των δεδομένων σε ένα ad-hoc δίκτυο. Απαιτεί από κάθε κόμβο να μεταδίδει περιοδικά αναπροσαρμοσμένες πληροφορίες δρομολόγησης στους άλλους κόμβους του δικτύου. Κάθε κινητός κόμβος στο δίκτυο, διατηρεί έναν πίνακα δρομολόγησης για όλους τους πιθανούς προορισμούς μέσα στο δίκτυο και τον αριθμό των απαιτούμενων συνδέσεων (hops) προς κάθε προορισμό. Κάθε καταχώρηση στον πίνακα αυτόν είναι μαρκαρισμένη με έναν αριθμό ακολουθίας, που ορίζεται από τον κόμβο προορισμού. Οι αριθμοί ακολουθίας επιτρέπουν στους κόμβους να διακρίνουν τις διαδρομές που είναι αποθηκευμένες και διατηρημένες στους πίνακες δρομολόγησης για μεγάλο χρονικό διάστημα, από τις καινούριες διαδρομές, αποφεύγοντας, παράλληλα, με τον τρόπο αυτόν την δημιουργία βρόχων στα μονοπάτια δρομολόγησης. Περιοδικά, σε όλους τους κόμβους του δικτύου, μεταδίδονται ανανεωμένες πληροφορίες δρομολόγησης με σκοπό την διατήρηση της συνέπειας των δεδομένων που βρίσκονται αποθηκευμένα στους πίνακες δρομολόγησης στους κόμβους του ad-hoc δικτύου.

Για να αποτρέψουν την κυκλοφορία στο δίκτυο μεγάλου όγκου πληροφοριών δρομολόγησης, οι αναπροσαρμογές των διαδρομών μπορούν να χρησιμοποιήσουν δύο τύπους πακέτων για να προωθήσουν στους κόμβους του δικτύου τις νέες πληροφορίες, «πλήρεις μεταδόσεις όλων των καταχωρήσεων ενός πίνακα ή επιλεκτικές μεταδόσεις των νέων καταχωρήσεων των πινάκων δρομολόγησης». Στην πρώτη περίπτωση δημιουργούνται μηνύματα πακέτων που μεταφέρουν όλες τις διαθέσιμες πληροφορίες δρομολόγησης, χρησιμοποιώντας πολλαπλές μονάδες δεδομένων (network protocol data units, NPDUs) για την μετάδοση των πληροφοριών. Τα πακέτα αυτά μεταδίδονται σπάνια και συνήθως κατά την περίοδο μετακίνησης των κόμβων του δικτύου. Στην δεύτερη περίπτωση μεταδίδονται μηνύματα, που περιέχουν μόνο εκείνες τις πληροφορίες δρομολόγησης που έχουν αλλάξει από την τελευταία μετάδοση όλων των καταχωρήσεων των πινάκων δρομολόγησης. Κάθε μια από αυτές τις μεταδόσεις πρέπει να μπορεί να χρησιμοποιήσει ένα συγκεκριμένο μέγεθος πακέτων NPDU, ούτως ώστε με τον τρόπο αυτό να μειωθεί ο όγκος της κυκλοφορίας που παράγεται. Οι κινητοί κόμβοι διατηρούν έναν πρόσθετο πίνακα όπου αποθηκεύουν τα δεδομένα δρομολόγησης που περιέχονται στα μηνύματα των καινούριων μεταδιδόμενων πληροφοριών δρομολόγησης. Οι μεταδόσεις διαδρομών δρομολόγησης περιέχουν τη διεύθυνση του προορισμού, τον αριθμό των συνδέσεων που απαιτούνται για να φθάσουν στον προορισμό τους, καθώς επίσης και έναν νέο αριθμό μοναδικό για τη κάθε μετάδοση. Η διαδρομή που επιλέγεται να χρησιμοποιηθεί είναι αυτή που περιέχει τον πιο πρόσφατο αριθμό ακολουθίας. Σε περίπτωση που υπάρχουν διαδρομές με τον ίδιο αριθμό ακολουθίας, η διαδρομή με μικρότερο μήκος χρησιμοποιείται ως βέλτιστη.

Οι κόμβοι επίσης παρακολουθούν το χρόνο εγκαθίδρυσης των διαδρομών ή το μέσο σταθμισμένο χρόνο αναμονής των διαδρομών που παραλαμβάνονται για έναν προορισμό, προτού παραληφθεί η καλύτερη διαδρομή. Με τον τρόπο αυτό καθυστερούν την μετάδοσης πληροφοριών δρομολόγησης, μειώνοντας την κυκλοφορία του δικτύου, περιμένοντας να μεταδώσουν διαδρομές που θα μπορούσαν να είναι υποψήφιες για να επιλέγουν, δηλαδή οι κόμβοι αποφεύγουν να μεταδώσουν μια διαδρομή αν πιστεύουν ότι στο άμεσο μέλλον από ένα άλλο κόμβο υπάρχει πολύ μεγαλύτερη πιθανότητα να μεταδοθεί μια καλύτερη διαδρομή.

2) The Wireless Routing Protocol: Το ασύρματο πρωτόκολλο δρομολόγησης (WRP) είναι ένα πρωτόκολλο που βασίζεται σε πίνακες δρομολόγησης με στόχο την εύρεση και διατήρηση πληροφοριών δρομολόγησης μεταξύ όλων των κόμβων του δικτύου. Κάθε κόμβος στο δίκτυο είναι αρμόδιος για τη διατήρηση τεσσάρων πινάκων: του πίνακα απόστασης, του πίνακας δρομολόγησης, του πίνακα κόστους των συνδέσεων των κόμβων και τέλος ενός πίνακα που περιέχει ένα κατάλογο μηνυμάτων αναμετάδοσης (Message Retransmission List MRL). Κάθε καταχώρηση του MRL περιέχει τον αριθμό ακολουθίας του μηνύματος ενημέρωσης ενός μετρητή αναμετάδοσης, ενός διανύσματος καταχωρήσεων απαιτήσεων επιβεβαιώσεων, μίας για κάθε γειτονικό κόμβο, και ενός καταλόγου ενημερώσεων διαδρομών που περιέχονται στα μηνύματα ενημέρωσης. Για την μετάδοση από ένα κόμβο των αρχείων του MRL στους γείτονες του, μέσω ενός μηνύματος ενημέρωσης, είναι απαραίτητο να λάβει από κάθε κόμβο επιβεβαίωση της ορθής τους μετάδοσης.

Οι κόμβοι ενημερώνουν ο ένας τον άλλο για τις αλλαγές των συνδέσεων μεταξύ τους, λόγω της κινητικότητας, μέσω της χρήσης των μηνυμάτων ενημέρωσης. Ένα μήνυμα ενημέρωσης στέλνεται μόνο μεταξύ γειτονικών κόμβων και περιέχει έναν κατάλογο αναπροσαρμογών (με τον προορισμό, την απόσταση από τον προορισμό, και τον προκάτοχο του προορισμού), καθώς επίσης και έναν κατάλογο με τους κόμβους που πρέπει να απαντήσουν με μια επιβεβαίωση παραλαβής των δεδομένων αυτών (Acks). Μετά την επεξεργασία των νέων πληροφοριών δρομολόγησης από τους γείτονες ή την ανίχνευση μιας αλλαγής σε μια σύνδεση, στέλνονται μηνύματα αναπροσαρμογών στους γείτονες κόμβους, περιέχοντας τις αλλαγές που έχουν ανακαλυφθεί. Σε περίπτωση απώλειας μιας σύνδεσης μεταξύ δύο κόμβων, οι κόμβοι στέλνουν μηνύματα ενημέρωσης στους γείτονές τους. Οι γείτονες τροποποιούν έπειτα τις καταχωρήσεις τους και ελέγχουν για νέες πιθανές διαδρομές μέσω άλλων κόμβων, για κάθε πιθανό προορισμό. Οποιεσδήποτε νέες πορείες ανακαλυφθούν, μεταδίδονται και αυτές, έτσι ώστε να μπορούν να ενημερώσουν τους πίνακές τους και οι υπόλοιποι κόμβοι του δικτύου, αναλόγως.

Οι κόμβοι μαθαίνουν για την ύπαρξη των γειτόνων τους από την παραλαβή των μηνυμάτων επιβεβαιώσεων ή άλλων μηνυμάτων. Εάν ένας κόμβος δεν μεταδίδει τέτοια μηνύματα, πρέπει να στείλει ένα (HELLO) μήνυμα εντός ενός καθορισμένου χρονικού διαστήματος, για να εξασφαλίσει την διασύνδεση με τους γείτονες του. Διαφορετικά, η έλλειψη μηνυμάτων οποιοδήποτε τύπου από κάποιο κόμβο, δείχνει αποτυχία για εκείνη τη σύνδεση, γεγονός που μπορεί να προκαλέσει ένα λάθος συναγερμό. Όταν ένας κόμβος λαμβάνει ένα (HELLO) μήνυμα από έναν νέο κόμβο του δικτύου, ο νέος κόμβος προστίθεται στον πίνακα δρομολόγησης και λαμβάνει ένα αντίγραφο των πινάκων δρομολόγησής του κόμβου στον οποίο έστειλε αρχικά το (HELLO) μήνυμα.

Μία σημαντική καινοτομία του WRP είναι ο τρόπος με τον οποίο επιτυγχάνει την απομάκρυνση των κυκλικών βρόχων στις διαδρομές δρομολόγησης. Οι κόμβοι που συμμετέχουν στη διαδικασία δρομολόγησης επιβάλλεται να εκτελούν ελέγχους συνέπειας με τις παλιότερες πληροφορίες δρομολόγησης για κάθε διαδρομή, που αναφέρονται από όλους τους γείτονές τους, με αποτέλεσμα να εξαλείφουν οποιουσδήποτε κυκλικές διαδρομές. Ταυτόχρονα παρέχουν την δυνατότητα διόρθωσης μιας διαδρομής μετά από την αποτυχία μίας σύνδεσης πάνω σε αυτή.[15]

2.4 Reactive Πρωτόκολλα Δρομολόγησης (On - Demand)

1) Δυναμική Δρομολόγηση Πηγής (Dynamic Source Routing): Ο δυναμικός αλγόριθμος δρομολόγησης πηγής (DSR) είναι μια καινοτόμα προσέγγιση στη δρομολόγηση ενός MANET, στην οποία οι κόμβοι επικοινωνούν χρησιμοποιώντας διαδρομές πηγής, που συμπεριλαμβάνονται στα πακέτα δεδομένων και τις οποίες χρησιμοποιούν οι ενδιάμεσοι κόμβοι για να τα προωθήσουν από τον κόμβο προέλευσης στον κόμβο προορισμού. Αναφέρεται ως ένα από τα καλά παραδείγματα reactive πρωτοκόλλου δρομολόγησης. Στον DSR, οι κινητοί κόμβοι διατηρούν Route Caches που περιέχουν καταχωρημένες τις διαδρομές πηγής τις οποίες ο κάθε κόμβος γνωρίζει. Οι καταχωρήσεις στην Route Cache ενημερώνονται συνεχώς καθώς νέες διαδρομές ανακαλύπτονται. Το πρωτόκολλο αποτελείται από δύο μηχανισμούς: τον μηχανισμό εύρεσης διαδρομών και τον μηχανισμό συντήρησης διαδρομών.

Όταν ένας κόμβος επιθυμεί να αποστείλει κάποια δεδομένα, αρχικά προσπαθεί να χρησιμοποιήσει μια διαδρομή που πιθανόν υπάρχει ήδη στην Route Cache του. Εάν μια ισχύουσα διαδρομή για τον συγκεκριμένο προορισμό υπάρχει, θα χρησιμοποιήσει αυτήν την διαδρομή για να μεταδώσει τα δεδομένα. Εάν όμως μια τέτοια διαδρομή δεν υπάρχει στην Route Cache, ενεργοποιείται η διαδικασία εύρεσης διαδρομών με τη μετάδοση ενός μηνύματος αιτήματος μιας νέας διαδρομής. Το μήνυμα αυτό περιέχει τη διεύθυνση προορισμού, μαζί με τη διεύθυνση του κόμβου προέλευσης και έναν μοναδικό αριθμό αναγνώρισης. Κάθε κόμβος που λαμβάνει το πακέτο ελέγχει εάν έχει αποθηκευμένη μια ισχύουσα διαδρομή για τον συγκεκριμένο προορισμό. Εάν όχι, προσθέτει τη διεύθυνσή του στο πεδίο διευθύνσεων των κόμβων διέλευσης του πακέτου και προωθεί το μήνυμα στους γειτονικούς του κόμβους. Για να περιοριστεί ο αριθμός των μηνυμάτων που διαδίδονται από κάθε κόμβο, ένας κόμβος μεταδίδει ένα τέτοιο μήνυμα μόνο εάν το λάβει για πρώτη φορά και δεν υπάρχει ήδη η διεύθυνση του στο πεδίο διευθύνσεων των κόμβων που έχει επισκεφτεί το μήνυμα. Μια απάντηση σε ένα αίτημα εύρεσης μιας διαδρομής παράγεται, είτε όταν παραληφθεί το εν λόγω μήνυμα από τον κόμβο προορισμού, είτε όταν ένας ενδιάμεσος κόμβος περιέχει στην Route Cache του μια ισχύουσα διαδρομή προς τον προορισμό. Στο πακέτο αποθηκεύεται όλη η αλληλουχία κόμβων από την οποία έχει περάσει το πακέτο, έως ότου φτάσει στον κόμβο προορισμού ή σε έναν ενδιάμεσο κόμβο και δημιουργηθεί μια απάντηση διαδρομής (Route Reply).

Η συντήρηση διαδρομών πραγματοποιείται μέσω της χρήσης πακέτων λαθών (Route Error) σε διαδρομές και των πακέτων επιβεβαιώσεων. Τα πακέτα (Route Error) παράγονται σε έναν κόμβο όταν παρουσιαστεί πρόβλημα στην μετάδοση των δεδομένων στο επίπεδο συνδέσεων του δικτύου. Όταν ένα τέτοιο πακέτο παραληφθεί, η καταχωρημένη διαδρομή στην οποία παρουσιάστηκε το λάθος, καθώς και όλες οι άλλες, που περιέχουν το σύνδεσμο στον οποίο παρουσιάστηκε το πρόβλημα, αφαιρούνται από την Route Cache του κόμβου. Τα πακέτα επιβεβαιώσεων, εν αντιθέσει, καθώς και τα πακέτα παθητικών επιβεβαιώσεων χρησιμοποιούνται για να ελέγξουν τη σωστή λειτουργία των συνδέσεων του δικτύου.

2) The Ad Hoc On-Demand Distance Vector Routing Protocol:Το πρωτόκολλο δρομολόγησης (AODV) είναι ένας συνδυασμός του πρωτοκόλλου DSDV και του DSR. Δανείζεται το βασικό μηχανισμό ανακάλυψης διαδρομών και συντήρησης διαδρομών από τον DSR και τη χρήση της δρομολόγησης μέσω των συνδέσεων (hop-by-hop), τους αριθμούς ακολουθίας και τα περιοδικά αναγνωριστικά μηνύματα από τον DSDV. Ο AODV ελαχιστοποιεί τον αριθμό των αναγκαίων μεταδόσεων με την εύρεση διαδρομών μόνο κατόπιν παραγγελίας, σε αντιδιαστολή με τη διατήρηση ενός πλήρους καταλόγου διαδρομών προς κάθε πιθανό προορισμό του δικτύου όπως συμβαίνει στον αλγόριθμο DSDV. Ο AODV ταξινομείται ως ένας αλγόριθμος δρομολόγησης που λειτουργεί εξ' ολοκλήρου on-demand, δεδομένου ότι οι κόμβοι, που δεν ανήκουν σε μια συγκεκριμένη διαδρομή, δεν διατηρούν πληροφορίες δρομολόγησης γι' αυτή και δεν συμμετέχουν στη ανταλλαγή πληροφοριών από πίνακες δρομολόγησης. Ο AODV υποστηρίζει μόνο συμμετρικές συνδέσεις και αποτελείται από δύο διαφορετικές φάσεις:

- Ανακάλυψη διαδρομών, συντήρηση διαδρομών, και

- Αποστολή δεδομένων.

Όταν ένας κόμβος επιθυμεί να στείλει ένα μήνυμα και δεν έχει ήδη μια έγκυρη διαδρομή προς τον προορισμό, ενεργοποιεί την διαδικασία εύρεσης διαδρομών για να εντοπίσει

τον αντίστοιχο κόμβο προορισμού. Μεταδίδει ένα μήνυμα αιτήματος διαδρομών (RREQ) στους γείτονές του, οι οποίοι το διαβιβάζουν στους δικούς τους γείτονές και ούτως καθ' εξής, μέχρι το αίτημα να προσεγγίσει είτε τον κόμβο προορισμού, είτε έναν ενδιάμεσο κόμβο με μια ισχύουσα διαδρομή προς τον προορισμό. Ο AODV χρησιμοποιεί αριθμούς ακολουθίας για κάθε προορισμό για να εξασφαλίσει ότι όλες οι διαδρομές δεν περιέχουν βρόχους και περιγράφουν τις πιο πρόσφατες πληροφορίες δρομολόγησης. Κάθε κόμβος διατηρεί τον αριθμό ακολουθίας του, καθώς επίσης και ένα μοναδικό αριθμό ταυτότητας για κάθε μετάδοση, ο οποίος αυξάνεται για κάθε (RREQ) που ο κόμβος στέλνει και μαζί με τη διεύθυνση IP του κόμβου προσδιορίζει μοναδικά κάθε ξεχωριστή μετάδοση δεδομένων προς έναν προορισμό. Μαζί με τον αριθμό ακολουθίας του κόμβου και του μοναδικού αριθμού μετάδοσης για τον συγκεκριμένο προορισμό, το RREQ περιλαμβάνει τον πιο πρόσφατο αριθμό ακολουθίας για τον προορισμό. Οι ενδιάμεσοι κόμβοι μπορούν να απαντήσουν στο RREQ μόνο εάν έχουν μια διαδρομή προς τον προορισμό της οποίας ο αντίστοιχος αριθμός ακολουθίας είναι μεγαλύτερος ή ίσος με αυτόν που υπάρχει στο μήνυμα αιτήματος. Κατά τη διάρκεια της διαδικασίας της εύρεσης μιας διαδρομής, οι ενδιάμεσοι κόμβοι στη διαδρομή καταγράφουν στους πίνακες δρομολόγησης τους τις διευθύνσεις του γείτονα από τον οποίο το πρώτο μήνυμα παραλήφθηκε. Με τον τρόπο αυτόν καθιερώνουν μια αντίστροφη διαδρομή προς τον κόμβο προορισμού του μηνύματος. Τα αντίγραφα του ίδιου RREQ, που πιθανώς να παραληφθούν αργότερα, απορρίπτονται. Μόλις το RREQ φθάσει στον προορισμό ή σε έναν ενδιάμεσο κόμβο με μια ισχύουσα διαδρομή, ο κόμβος αυτός δημιουργεί ένα πακέτο απάντησης (RREP), το οποίο μεταδίδει πίσω στον κόμβο από τον οποίο έλαβε αρχικά το RREQ. Δεδομένου ότι το RREP καθοδηγείται πίσω κατά μήκος της αντίστροφης διαδρομής που έχει δημιουργηθεί από τους ενδιάμεσους κόμβους, οι κόμβοι κατά μήκος της πορείας αυτής, καθώς προωθούν, το πακέτο οργανώνουν τις προς τα εμπρός καταχωρήσεις μονοπατιών στους πίνακες δρομολόγησης τους, που δείχνουν τον κόμβο από τον οποίο το RREP προήλθε. Αυτές οι καταχωρήσεις διαδρομών περιγράφουν την ενεργό διαδρομή δρομολόγησης του συγκεκριμένου RREP. Σε κάθε καταχώρηση μιας διαδρομής στους πίνακες δρομολόγησης αντιστοιχεί ένας χρόνος ζωής διαδρομών, που προκαλεί τη διαγραφή τους από τους πίνακες, εάν αυτές δεν χρησιμοποιηθούν μέσα στο συγκεκριμένο χρονικό διάστημα. Ο λόγος για τον οποίο ο AODV υποστηρίζει μόνο συμμετρικές συνδέσεις είναι ότι το RREP διαβιβάζεται κατά μήκος της πορείας που δημιουργείται από το RREQ.

Οι διαδρομές στον AODV διατηρούνται ως εξής, στις περιπτώσεις που κάποιος κόμβος κατά μήκος της διαδρομής κινείται με αποτέλεσμα η διαδρομή αυτή να μην ισχύει πλέον. Όταν ένας κόμβος προέλευσης μιας διαδρομής κινείται, είναι σε θέση να ενεργοποιήσει ξανά τον μηχανισμό εύρεσης διαδρομών για να ανακαλύψει μια νέα διαδρομή προς τον προορισμό. Εάν ένας κόμβος κατά μήκος της διαδρομής κινείται, ο προς τα πάνω (upstream) γείτονάς του παρατηρεί την κίνηση του και διαδίδει ένα μήνυμα ανακοίνωσης αποτυχίας της σύνδεσης (RREP with infinite metric) σε κάθε ένας από τους ενεργούς προς τα πάνω (upstream) γείτονές του, για να τους ενημερώσει για τη κατάρρευση του συγκεκριμένου μέρους της διαδρομής. Οι κόμβοι αυτοί διαδίδουν στη συνέχεια το μήνυμα κατάρρευσης των συνδέσεων στους προς τα πάνω γείτονές τους και η διαδικασία αυτή συνεχίζεται έως ότου το μήνυμα το λάβει ο κόμβος πηγή της συγκεκριμένης διαδρομής. Ο κόμβος αυτός έπειτα ενεργοποιεί, αν το κρίνει απαραίτητο και αναγκαίο να διατηρήσει μια διαδρομή για τον συγκεκριμένο προορισμό, τον μηχανισμό εύρεσης διαδρομών του πρωτοκόλλου. Ένα ακόμα χαρακτηριστικό του πρωτοκόλλου είναι η χρήση μηνυμάτων (HELLO), με περιοδικές τοπικές μεταδόσεις

από έναν κόμβο για να ενημερώσει κάθε άλλο κινούμενο κόμβο για την παρουσία άλλων κόμβων στην περιοχή εμβέλειας του. Τα μηνύματα αυτά μπορούν να χρησιμοποιηθούν για να διατηρήσουν την τοπική συνδεσιμότητα ενός κόμβου με τους γείτονες του. Εντούτοις, η χρήση αυτών των μηνυμάτων δεν είναι απαραίτητη σε όλες τις περιπτώσεις, αφού οι κόμβοι «ακούγοντας» τις αναμεταδώσεις των πακέτων δεδομένων μπορούν να εξασφαλίσουν την διασύνδεση τους με τους γειτονικούς τους κόμβους. Γενικά τόσο από τα πακέτα δεδομένων που προωθούνται από έναν κόμβο ή μπορούν να ληφθούν χωρίς να προορίζονται γι' αυτόν, όσο και ειδικά μηνύματα, όπως τα (HELLO) μηνύματα, χρησιμοποιούνται για να μπορούν οι κόμβοι ενός ad-hoc δικτύου να αποκτούν μια όσο το δυνατόν καλύτερη εικόνα για το ίδιο το δίκτυο, τους γείτονες τους και τις ενεργές συνδέσεις τους.

3) Associativity Based Routing: Το πρωτόκολλο ABR, είναι μια διαφορετική προσέγγιση στην δρομολόγηση ad-hoc ασύρματων δικτύων. Στις διαδρομές που ανακαλύπτει είναι απαλλαγμένο από βρόχους, αδιέξοδα (deadlocks), παραλαβή διπλών πακέτων και καθορίζει μια νέα τεχνική δρομολόγησης για τα ad-hoc ασύρματα δίκτυα. Στο ABR, μια διαδρομή επιλέγεται βασιζόμενη σε ένα παράγοντα που είναι γνωστός ως βαθμός συσχέτισης της ευστάθειας (degree of association stability). Κάθε κόμβος παράγει περιοδικά ένα αναγνωριστικό μήνυμα για να δηλώσει την ύπαρξή του στους υπόλοιπους κόμβους του δικτύου. Όταν το μήνυμα αυτό παραλαμβάνεται από τους γειτονικούς κόμβους, αναγκάζει τους πίνακες συσχέτισης να ενημερωθούν. Η συσχέτιση της ευστάθειας καθορίζεται από τη σταθερότητα σύνδεσης ενός κόμβου όσον αφορά έναν άλλο κόμβο στο χρόνο και στο χώρο. Ένας υψηλός (χαμηλός) βαθμός συσχέτισης της ευστάθειας μπορεί να δείξει μια χαμηλή (υψηλή) κατάσταση κινητικότητας των κόμβων. Οι δείκτες καταγραφής ρυθμίζονται ξανά όταν κινούνται οι γείτονες ενός κόμβου ή ο ίδιος ο κόμβος απομακρύνεται. Ένας θεμελιώδης στόχος είναι να παραχθούν διαδρομές που έχουν μεγάλο χρόνο ζωής για τα ειδικά δίκτυα. Οι τρεις φάσεις του ABR είναι: Ανακάλυψη διαδρομών, Αναδημιουργία διαδρομών (RRC) και Διαγραφή διαδρομών.

Η φάση ανακάλυψης διαδρομών υλοποιείται από μια συνεχή διαδικασία μετάδοσης μιας ερώτησης και αναμονή μιας απάντησης (Broadcast Query Reply, BQ-REPLY). Ένας κόμβος που επιθυμεί μια διαδρομή μεταδίδει ένα μήνυμα BQ σε αναζήτηση των κόμβων που έχουν μια διαδρομή προς τον προορισμό. Όλοι οι κόμβοι που λαμβάνουν την ερώτηση (χωρίς να είναι ο τελικός προορισμός του μηνύματος) επισυνάπτουν τις διευθύνσεις τους και τους δείκτες συσχέτισης τους, σε σχέση με τους γείτονές τους, μαζί με πληροφορίες ποιότητας των συνδέσεων QoS στο πακέτο ερώτησης. Ο κόμβος στον οποίο προωθείται το μήνυμα σβήνει τις καταχωρήσεις των δεικτών συσχέτισης των προς τα πάνω γειτόνων κόμβων του και διατηρεί μόνο αυτές τις καταχωρίσεις που συσχετίζονται με αυτόν και τους κόμβους που είναι αντίθετα με την κατεύθυνση προώθησης του μηνύματος. Κατ' αυτό τον τρόπο, κάθε πακέτο που φθάνει στον προορισμό περιέχει τους δείκτες συσχέτισης των κόμβων κατά μήκος της διαδρομής. Ο κόμβος προορισμού έπειτα είναι ικανός να επιλέξει την καλύτερη διαδρομή με την εξέταση των δεικτών συσχέτισης κατά μήκος κάθε μίας από τις διαδρομές. Όταν οι πολλαπλές διαδρομές έχουν τον ίδιο γενικό βαθμό συσχέτισης ευστάθειας, η διαδρομή με τον ελάχιστο αριθμό συνδέσμων επιλέγεται. Ο προορισμός στέλνει έπειτα ένα πακέτο απάντησης πίσω στον κόμβο προέλευσης. Οι κόμβοι που προωθούν το μήνυμα αυτό χαρακτηρίζουν τις διαδρομές τους ως έγκυρες. Όλες οι άλλες διαδρομές παραμένουν ανενεργές, με αποτέλεσμα να αποφεύγεται η αποστολή διπλών πακέτων να φθάνουν στον προορισμό.

2.5 Flow Oriented Routing

1) Relative Distance Micro Discovery Ad-Hoc Routing: Το πρωτόκολλο δρομολόγησης RDMAR είναι ένα ιδιαίτερα προσαρμοστικό και αποδοτικό πρωτόκολλο. Μπορεί να λειτουργήσει αρκετά ικανοποιητικά σε μεγάλα ασύρματα ad-hoc δίκτυα στα οποία παρατηρείται μέτρια κινητικότητα. Βασική σχεδιαστική αρχή του πρωτοκόλλου είναι η αντίδραση του στην διακοπή της ενεργής λειτουργίας αποτυχημένων συνδέσεων, σε μια πολύ μικρή περιοχή του δικτύου κοντά στο σημείο της αλλαγής των συνδέσεων του δικτύου. Η συμπεριφορά αυτή επιτυγχάνεται μέσω της χρήσης ενός νέου μηχανισμού για την ανακάλυψη διαδρομών, αποκαλούμενου Relative Distance Micro-Discovery (RDM), ο οποίος έχει σαν βασικής έννοια την δημιουργία μηνυμάτων, ως αντίδρασης του πρωτοκόλλου σε ένα γεγονός και την διάδοση τους με την μορφή πλημμύρας, η οποία μπορεί να περιοριστεί χρησιμοποιώντας την σχετική απόσταση (RD) μεταξύ δύο τερματικών. Κάθε φορά που προκαλείται μια αναζήτηση διαδρομών μεταξύ των δύο τερματικών, ένας επαναληπτικός αλγόριθμος υπολογίζει μια εκτίμηση της σχετικής τους απόστασης, λαμβάνοντας υπόψη ένα μέσο ρυθμό κινητικότητας, πληροφορίες για την περίοδο που έχει παρέλθει από την πιο πρόσφατη επικοινωνίας τους και τις προηγούμενες τιμές της. Το μήνυμα ερώτησης (query) το οποίο δημιουργείται βασισμένο στο υπολογισμένο αυτό RD, προωθείται με την τεχνική της πλημμύρας σε όλους του κόμβους του δικτύου σε μια περιοχή η οποία κεντροθετείται στον κόμβο πηγής του αιτήματος ευρέσεως διαδρομών και με μέγιστη ακτίνα διάδοσης ίση με την κατ' εκτίμηση σχετική απόσταση RD. Η παραπάνω διαδικασία χρησιμεύει για να ελαχιστοποιηθεί η συμφόρηση του δικτύου και η συνολική καθυστέρηση που προκαλείται από το πρωτόκολλο δρομολόγησης.

Στο RDMAR, τα δεδομένα δρομολογούνται μεταξύ των κόμβων του δικτύου με τη χρησιμοποίηση πινάκων δρομολόγησης αποθηκευμένων σε κάθε κόμβο. Κάθε κόμβος έχει το ρόλο τόσο του τερματικού όσο και του δρομολογητή. Κάθε πίνακας δρομολόγησης περιέχει πληροφορίες για όλους ξεχωριστά τους πιθανούς προορισμούς στο δίκτυο. Κάθε καταχώρηση στον πίνακα αυτόν περιέχει τον επόμενο κόμβο, στον οποίο πρέπει να μεταδοθούν τα δεδομένα για να μπορέσουν να προωθηθούν στον τελικό προορισμό τους. Η σχετική απόσταση (Relative Distance RD) περιέχει μια προσέγγιση της απόστασης, εκφρασμένη σε πλήθος συνδέσεων (hops), ανάμεσα στον κόμβο αυτό και τον κόμβο προορισμού και τον χρόνο (Time Last Update TLU) από την τελευταία φορά που ο κόμβος είχε λάβει πληροφορίες δρομολόγησης για τον συγκεκριμένο προορισμό. Μία μεταβλητή που ονομάζεται (RT_Timeout) περιέχει το χρονικό διάστημα που απομένει προτού θεωρηθεί η συγκεκριμένη διαδρομή άκυρη και τέλος έναν αναγνωριστικό αριθμό που (Route Flag), που δηλώνει εάν η διαδρομή είναι ενεργή. Ο RDMAR περιλαμβάνει δύο κύριους μηχανισμούς:

- Εύρεση διαδρομών — Όταν φθάνει μια αίτηση σε έναν κόμβο για μια διαδρομή προς ένα άλλο κόμβο και δεν υπάρχει διαθέσιμη κάποια διαδρομή, ενεργοποιείται ο μηχανισμός εύρεσης διαδρομών του πρωτοκόλλου. Το μήνυμα αίτησης για την νέα διαδρομή μπορεί, είτε να διαδοθεί με την τεχνική της πλημμύρας σε όλους του κόμβους του δικτύου, είτε να περιοριστεί η μετάδοση του μηνύματος σε μια συγκεκριμένη περιοχή, βάση μιας πρόβλεψης της θέσης του κόμβου προορισμού, που γίνεται με τον υπολογισμό μιας πρόβλεψης, για την απόσταση του κόμβου προορισμού από τις πληροφορίες που υπάρχουν στους πίνακες δρομολόγησης.

- Συντήρηση διαδρομών — Ένας ενδιάμεσος κόμβος, κατά την υποδοχή ενός πακέτου δεδομένων, επεξεργάζεται αρχικά τις πληροφορίες δρομολόγησης και τις διαβιβάζει έπειτα στον επόμενο κόμβο. Στη συνέχεια μεταδίδει ένα μήνυμα με σκοπό να εξετάζει εάν μια αμφίδρομη σύνδεση, με ένα προηγούμενο κόμβο, είναι εφικτή. Ο RDMAR επομένως, δεν υποθέτει την ύπαρξη αμφίδρομων συνδέσεων αλλά παρόλα αυτά εξετάζει τη δυνατότητα αυτή. Κατά τον τρόπο αυτό, οι κόμβοι που προωθούν ένα πακέτο δεδομένων έχουν πάντα αρκετές πληροφορίες δρομολόγησης για να στείλουν ένα μελλοντικό πακέτο επιβεβαίωσης πίσω στην πηγή. Εάν η προώθηση του πακέτου δεδομένων, είτε λόγω κάποιου λάθους που υπάρχει στις συνδέσεις της διαδρομής, είτε λόγω του ότι δεν υπάρχει καμία διαθέσιμη διαδρομή, αποτύχει, η διαδικασία επαναλαμβάνεται μέχρι έναν μέγιστο αριθμό και στη συνέχεια εάν η αποτυχία εμμένει, ενεργοποιείται η διαδικασία εύρεσης διαδρομών.

2) Signal Stability Routing (SSR): Είναι ένα on-demand πρωτόκολλο δρομολόγησης. Αντίθετα από τους αλγορίθμους που περιγράφηκαν μέχρι τώρα, το SSR επιλέγει διαδρομές βασισμένες στην ισχύ των σημάτων των ασύρματων πομποδεκτών μεταξύ των κόμβων και στην σταθερότητα διατήρησης της θέσης από τους κόμβους του δικτύου. Οι εντάσεις των σημάτων των γειτονικών κόμβων λαμβάνονται από περιοδικά αναγνωριστικά μηνύματα από το επίπεδο συνδέσεων κάθε κόμβου. Αυτό το κριτήριο επιλογής διαδρομών SSR έχει την επίδραση της επιλογής διαδρομών που αποτελούνται από συνδέσεις που έχουν «stronger connectivity).

2.6 Πρωτόκολλα Adaptive Routing (Situation-Aware) - Δρομολόγηση Αναστροφής Συνδέσεων

Στην παράγραφο αυτή θα περιγράψουμε το σημαντικότερο πρωτόκολλο αυτής της οικογένειας το οποίο ονομάζεται TORA (Temporally Ordered Routing Algorithm).

Ο αλγόριθμος δρομολόγησης (TORA) είναι ένας ιδιαίτερα προσαρμοστικός, κατανεμημένος αλγόριθμος βασισμένος στην έννοια της αντιστροφής συνδέσεων, ο οποίος διαθέτει ειδικό μηχανισμό εξάλειψης βρόγχων μέσα στις διαδρομές, έχοντας ως σκοπό την ελαχιστοποίηση των αντιδράσεων στις τοπολογικές αλλαγές του δικτύου.

Μια βασική σχεδιαστική αρχή του αλγορίθμου είναι ότι προσπαθεί να αντιμετωπίσει την κινητικότητα και την αλλαγή της τοπολογία των κόμβων, απομονώνοντας τους κόμβους του δικτύου που δεν αφορά ούτε και επηρεάζει αυτή η αλλαγή. Αυτό έχει σαν αποτέλεσμα οι τυχών αλλαγές στην τοπολογία του δικτύου που συμβαίνουν σε μια συγκεκριμένη περιοχή να επηρεάζουν μια μικρή ομάδα κοντινών κόμβων και όχι τους απομακρυσμένους. Η ανταλλαγή μηνυμάτων ελέγχου δρομολόγησης λοιπόν σε μια περιορισμένη ομάδα κόμβων, που βρίσκονται κοντά στην αλλαγή, έχει ως αποτέλεσμα την καλύτερη απόδοση του πρωτοκόλλου και την αποφυγή χρήσης ιεραρχικών αλγορίθμων δρομολόγησης που θα προσέθεταν έξτρα πολυπλοκότητα. Η εύρεση των καλύτερων διαδρομών θεωρείται δευτερεύουσας σημασίας και πολύ συχνά δεν χρησιμοποιούνται οι βέλτιστες διαδρομές, εάν η διαδικασία εύρεσης νέων διαδρομών είναι δυνατόν να αποφευχθεί. Τέλος το πρωτόκολλο αυτό χαρακτηρίζεται και από την ικανότητα δρομολόγησης μέσω πολλαπλών διαδρομών.

Το TORA είναι ικανό να λειτουργήσει σε ένα ιδιαίτερα δυναμικό περιβάλλον όπως συνήθως είναι ένα ασύρματο ad-hoc δίκτυο με κινούμενους κόμβους. Η διαδικασία δρομολόγησης ξεκινά σε όλες τις περιπτώσεις από έναν κόμβο (source node). Οι κόμβοι πρέπει να διατηρούν τις πληροφορίες δρομολόγησης για τους παρακείμενους κόμβους (γειτονικούς κόμβους). Το πρωτόκολλο εκτελεί τρεις βασικές λειτουργίες:

- Δημιουργία διαδρομών,
- Συντήρηση διαδρομών, και
- Εξάλειψη διαδρομών.

Για κάθε κόμβο στο δίκτυο, ένας ξεχωριστός κατευθυνόμενος μη-κυκλικός γράφος (Directed Acyclic Graph DAG) διατηρείται για κάθε προορισμό. Όταν ένας κόμβος αποφασίσει ότι χρειάζεται μια διαδρομή για κάποιον προορισμό, διαδίδει προς όλους τους κόμβους του δικτύου ένα μήνυμα αναζήτησης (Query), που περιέχει τη διεύθυνση του προορισμού για τον οποίο απαιτεί μια διαδρομή. Αυτό το πακέτο προωθείται από κόμβο σε κόμβο, έως ότου φθάσει είτε στον κόμβο προορισμού, είτε σε έναν ενδιάμεσο κόμβο που έχει αποθηκευμένη μια διαδρομή προς τον προορισμό. Ο παραλήπτης του μηνύματος αυτού μεταδίδει ένα μήνυμα ενημέρωσης (Update), που απαριθμεί το ύψος που γνωρίζει σε σχέση με τον κόμβο προορισμού. Καθώς το μήνυμα αυτό προωθείται στο δίκτυο, κάθε κόμβος που το λαμβάνει ρυθμίζει το δικό του ύψος προς το συγκεκριμένο προορισμό κατά μία μονάδα μεγαλύτερο από το ύψος του γειτονικού του κόμβου από τον οποίο το έλαβε. Η διαδικασία αυτή έχει σαν αποτέλεσμα την δημιουργία μιας σειράς κατευθυνόμενων συνδέσεων από τον αρχικό αποστολέα της αναζήτησης της διαδρομής, προς τον κόμβο που παρήγαγε το μήνυμα ενημέρωσης (Update). Όταν ένας κόμβος αντιληφθεί ότι μια διαδρομή προς ένα συγκεκριμένο προορισμό δεν ισχύει πλέον, αναπροσαρμόζει το ύψος που έχει αποθηκεύσει γι' αυτή την διαδρομή στο μέγιστο που μπορεί να υπολογίσει από τις πληροφορίες που έχει συλλέξει από τους γείτονες του και διαδίδει στη συνέχει ένα μήνυμα (Update). Εάν ο κόμβος δεν έχει κάποιον γείτονα που μπορεί να τον πληροφορήσει για το ύψος προς τον συγκεκριμένο προορισμό, ενεργοποιεί την διαδικασία εύρεσης μιας νέας διαδρομής, όπως περιγράφεται ανωτέρω. Όταν ένας κόμβος ανιχνεύσει την κατάτμηση του δικτύου, δημιουργεί ένα μήνυμα καθαρίσματος (Clear) που ρυθμίζει εκ νέου την κατάσταση των διαδρομών και διαγράφει διαδρομές που πλέον δεν είναι ενεργές.

Το TORA είναι υλοποιημένο πάνω από το επίπεδο του IMEP το πρωτόκολλο ενθυλάκωσης των MANET, το οποίο εγγυάται τη με σειρά αξιόπιστη παράδοση όλων των μηνυμάτων ελέγχου της διαδικασίας της δρομολόγησης από έναν κόμβο σε κάθε ένα από τους γείτονές του και την ειδοποίηση για την δημιουργία μιας νέας ή την κατάργηση μιας παλιάς σύνδεσης με ένα γειτονικό κόμβο, στο επίπεδο του πρωτοκόλλου δρομολόγησης. Για να μειώσει την καθυστέρηση, το IMEP προσπαθεί να ομαδοποιήσει πολλά μηνύματα ελέγχου του TORA και του ίδιου του IMEP (τα οποία αναφέρονται ως αντικείμενα) σε ένα ενιαίο πακέτο πριν από κάθε μετάδοση. Κάθε τέτοιο πακέτο φέρνει έναν αριθμό ακολουθίας και έναν κατάλογο άλλων κόμβων από τους οποίους απαιτείται μία λήψη επιβεβαίωσης. Το IMEP μεταδίδει κάθε ίδιο τέτοιο πακέτο περιοδικά και συνεχίζει να το μεταδίδει, εάν είναι απαραίτητο, για κάποια περίοδο, μετά το πέρας της οποίας το TORA ενημερώνεται για όλες τις συνδέσεις που δεν ισχύουν πλέον, λόγω του ότι δεν έχει ληφθεί κάποια επιβεβαίωση.

Όπως αναφέραμε νωρίτερα, κατά τη διάρκεια της δημιουργίας και συντήρησης διαδρομών, οι κόμβοι χρησιμοποιούν το «ύψος» σαν μέτρο εγκαθίδρυσης ενός κατευθυντικού μη κυκλικού γράφου διαδρομών, (DAG) προς τον προορισμό. Στις συνδέσεις, μετά από αυτή τη διαδικασία, ορίζεται μια κατεύθυνση (προς τα πάνω ή προς τα κάτω) βασισμένη με το σχετικό ύψος των γειτονικών κόμβων. Σε περιόδους κινητικότητας των κόμβων ο γράφος διαδρομών DAG περιέχει μη συνεπείς πληροφορίες και η διαδικασία συντήρησης διαδρομών είναι απαραίτητη για να εγκαθιδρύσει ξανά ένα γράφο διαδρομών, ο οποίος περιέχει τις νέες πληροφορίες δρομολόγησης.

Ο συγχρονισμός είναι ένας σημαντικός παράγοντας στο πρωτόκολλο TORA, επειδή το «ύψος» εξαρτάται από το χρόνο αποτυχίας των συνδέσεων. Το TORA υποθέτει ότι όλοι οι κόμβοι έχουν συγχρονίσει τα ρολόγια τους, χρησιμοποιώντας μια αρκετά αξιόπιστη υπηρεσία συγχρονισμού, όπως είναι το GPS (Global Positioning System). Οι παράγοντες που χρησιμοποιούνται από το TORA σαν μέτρο για τις διαδικασίες δρομολόγησης και διατήρησης των διαδρομών είναι οι εξής πέντε:

1. Λογικός χρόνος αποτυχίας μιας σύνδεσης,
2. Η μοναδική ταυτότητα του κόμβου που καθόρισε το νέο επίπεδο αναφοράς,
3. Ένα bit που περιγράφει ένα δείκτη αντανάκλασης,
4. Μια παράμετρος διάδοσης,
5. Η μοναδική ταυτότητα του κόμβου.

Το TORA είναι ένα πρωτόκολλο μερικώς reactive και μερικώς proactive. Είναι reactive υπό την έννοια ότι η διαδικασία εύρεσης διαδρομών αρχίζει μετά από σχετική αίτηση κάποιου κόμβου. Εντούτοις, η συντήρηση των διαδρομών γίνεται proactive έτσι ώστε οι πολλαπλάσιες επιλογές δρομολόγησης να είναι διαθέσιμες και έγκυρες σε περίπτωση ύπαρξης αποτυχημένων συνδέσεων.[15]

2.7 Υβριδικά Πρωτόκολλα Δρομολόγησης

1) Πρωτόκολλο Δρομολόγησης Ζώνης (Zone Routing Protocol): Το πρωτόκολλο δρομολόγησης ζώνης (ZRP) είναι ένα υβριδικό παράδειγμα reactive και proactive δρομολόγησης. Περιορίζει το πεδίο της proactive διαδικασίας μόνο στην περιοχή όπου βρίσκονται οι γείτονες ενός κόμβου, ενώ η αναζήτηση σε όλο το δίκτυο μπορεί να εκτελεστεί αποτελεσματικά με τη αναζήτηση συγκεκριμένων κόμβων μετά από σχετικό αίτημα, όπως σε ένα reactive πρωτόκολλο.

Στο ZRP, ένας κόμβος διατηρεί proactively διαδρομές προς τους κόμβους προορισμούς μέσα σε μια περιοχή, η οποία αναφέρεται ως ζώνη δρομολόγησης και ορίζεται ως μια συλλογή των κόμβων, των οποίων η ελάχιστη απόσταση συνδέσεων από τον εν λόγω κόμβο δεν είναι μεγαλύτερη από μια παράμετρο, καλούμενη ακτίνα ζώνης. Κάθε κόμβος διατηρεί την ακτίνα ζώνης του. Από το πρωτόκολλο επιτρέπεται και επιβάλλετε να υπάρχει μια επικάλυψη γειτονικών ζωνών.

Η κατασκευή μιας ζώνης δρομολόγησης απαιτεί ένας κόμβος να γνωρίζει ποιοι είναι οι γείτονές του. Ένας γείτονας ορίζεται ως ένας κόμβος που μπορεί να επικοινωνήσει άμεσα με τον εν λόγω κόμβο και ανακαλύπτεται μέσω ενός πρωτοκόλλου ανακαλύψεως γειτόνων του επιπέδου MAC (Neighbor Discovery Protocol NDP). Το ZRP διατηρεί τις ζώνες δρομολόγησης μέσω ενός proactive πρωτοκόλλου καλούμενου (Intrazone Routing Protocol IARP), που υλοποιείται ως ένα τροποποιημένο διανυσματικό σχήμα απόστασης. Το πρωτόκολλο αυτό είναι αρμόδιο για την εύρεση των διαδρομών για τους

προορισμούς που βρίσκονται έξω από τη ζώνη δρομολόγησης. Το IERP χρησιμοποιεί έναν μηχανισμό ερώτησης και απάντησης (query-response) για να ανακαλύψει τις διαδρομές μετά από σχετική αίτηση κάποιου κόμβου. Το IERP διακρίνεται από τον κλασικό αλγόριθμο πλημμύρας λόγω της χρησιμοποίηση διαδικασίας προώθησης μηνυμάτων γνωστής ως border casting. Το ZRP παρέχει αυτήν την υπηρεσία μέσω μιας διεργασίας αποκαλούμενης, (Border Resolution Protocol BRP).

Το στρώμα δικτύου προκαλεί μία IERP ανακάλυψη διαδρομών όταν ένα πακέτο στοιχείων πρόκειται να σταλεί σε έναν προορισμό που δεν βρίσκεται μέσα στη ζώνη δρομολόγησής του. Η πηγή παράγει ένα μήνυμα αναζήτησης διαδρομών, το οποίο προσδιορίζεται μεμονωμένα από έναν αριθμό ταυτότητας και έναν αριθμό αιτήματος του κόμβου πηγής. Η ερώτηση έπειτα μεταδίδεται στους απομακρυσμένους κόμβους από την ζώνη δρομολόγησης. Κατά την παραλαβή ενός τέτοιου πακέτου, ένας κόμβος προσθέτει τον δικό του αριθμό ταυτότητας. Η ακολουθία των καταγραμμένων αριθμών αυτών διευκρινίζει μια διαδρομή από την πηγή στην τρέχουσα ζώνη δρομολόγησης. Εάν ο προορισμός δεν εμφανίζεται στη τρέχουσα ζώνη δρομολόγησης, το μήνυμα αυτό προωθείται στους απομακρυσμένους κόμβους της ζώνης δρομολόγησης. Εάν ο κόμβος προορισμού είναι μέλος της τρέχουσας ζώνης δρομολόγησης, αποστέλλεται πίσω στην πηγή μια απάντηση που περιέχει την συγκεκριμένη διαδρομή, ακολουθώντας απλά την αντίστροφη διαδρομή από αυτή που περιέχει. Ένας κόμβος θα απορρίψει οποιοδήποτε μήνυμα αναζήτησης διαδρομών, το οποίο έχει επεξεργαστεί ξανά. Ένα σημαντικό χαρακτηριστικό αυτής της διαδικασίας είναι ότι μια μοναδική αναζήτηση διαδρομών μπορεί να επιστρέψει πολλαπλές απαντήσεις με διαδρομές για τον προορισμό, δίνοντας την δυνατότητα επιλογής της καλύτερης από αυτές στους κόμβους, βάση κάποιων χαρακτηριστικών της ποιότητας τους.

2) Το πρωτόκολλο δρομολόγησης (LANMAR) συνδυάζει τα χαρακτηριστικά γνωρίσματα του FSR και της διαδικασίας δρομολόγησης Landmark. Η βασική καινοτομία είναι η χρήση ορόσημων για κάθε σύνολο κόμβων που κινούνται ως ομάδα (όπως, μια ομάδα στρατιωτών στο πεδίο της μάχης) προκειμένου να μειωθεί η συνολική καθυστέρηση δρομολόγησης. Όπως και στον FSR, οι κόμβοι ανταλλάσσουν πληροφορίες μόνο με τους γειτονικούς τους κόμβους. Οι διαδρομές στο πλαίσιο του Fisheye είναι ακριβείς, ενώ οι διαδρομές στις μακρινές ομάδες κόμβων «συνοψίζονται» (summarized) από τα αντίστοιχα ορόσημα. Ένα πακέτο που κατευθύνεται σε έναν μακρινό προορισμό στοχεύει αρχικά προς το αντίστοιχο ορόσημο της απομακρυσμένης ομάδας κόμβων και καθώς πλησιάζει πιο κοντά στον προορισμό χρησιμοποιεί τελικά μια πιο συγκεκριμένη διαδρομή που παρέχεται από το Fisheye. Στο αρχικό σχήμα ενσύρματων δικτύων με ορόσημα, η προκαθορισμένη διεύθυνση κάθε κόμβου απεικονίζει τη θέση του μέσα στην ιεραρχία και βοηθά την εύρεση μιας διαδρομής σε αυτόν. Κάθε κόμβος γνωρίζει τις διαδρομές προς όλους τους άλλους κόμβους μέσα στο ιεραρχικό σχήμα. Επιπλέον, κάθε κόμβος γνωρίζει τις διαδρομές προς τα διάφορα "ορόσημα" σε διαφορετικά ιεραρχικά επίπεδα. Η αποστολή πακέτων είναι σύμφωνη με την ιεραρχία ορόσημων και η πορεία καθορίζεται από την ιεραρχία υψηλότερου επιπέδου στα χαμηλότερα επίπεδα καθώς ένα πακέτο πλησιάζει προς τον προορισμό.

Το LANMAR δανείζεται την έννοια των ορόσημων για να παρακολουθήσει τα λογικά υποδίκτυα. Ένα υποδίκτυο αποτελείται από μέλη που έχουν κοινά ενδιαφέροντα και είναι πιθανόν να κινηθούν ως "ομάδα" (όπως, στρατιώτες στο πεδίο μάχης, ή μια ομάδα σπουδαστών). Ένας κόμβος "ορόσημων" εκλέγεται σε κάθε υποδίκτυο. Το ίδιο το σχέδιο δρομολόγησης είναι τροποποιημένη έκδοση του FSR. Η κύρια διαφορά όμως είναι ότι ο πίνακας δρομολόγησης του FSR περιέχει όλους τους κόμβους στο δίκτυο, ενώ ο πίνακας

δρομολόγησης στο LANMAR περιλαμβάνει μόνο τους κόμβους άμεσου ενδιαφέροντος και τους κόμβους ορόσημων (landmark nodes). Αυτό το χαρακτηριστικό γνώρισμα βελτιώνει πολύ την κλιμάκωση του πρωτοκόλλου με τη μείωση του μεγέθους των πινάκων δρομολόγησης και την συνολικής κυκλοφορίας των δεδομένων στο δίκτυο. Όταν ένας κόμβος πρέπει να αναμεταδώσει ένα πακέτο, εάν ο προορισμός είναι ένας από τους γείτονες του, η διεύθυνση βρίσκεται στον πίνακα δρομολόγησης και το πακέτο διαβιβάζεται άμεσα. Διαφορετικά, το υποδίκτυο που πιθανά βρίσκεται ο προορισμός αναζητάτε και το πακέτο καθοδηγείται προς το αντίστοιχο ορόσημο εκείνου του υποδικτύου. Το πακέτο εντούτοις δεν είναι αναγκαίο να περάσει μέσω του κόμβου ορόσημου αλλά μπορεί να προωθηθεί άμεσα στον προορισμό, μόλις φτάσει κοντά στο συγκεκριμένο υποδίκτυο.

Η ανταλλαγή ανανεωμένων πληροφοριών δρομολόγησης στο LANMAR είναι παρόμοια με του FSR. Κάθε κόμβος ανταλλάσσει περιοδικά πληροφορίες τοπολογίας με τους γείτονές του. Σε κάθε αναπροσαρμογή, ο κόμβος στέλνει τις νέες καταχωρήσεις στο πεδίο Fisheye του, συμπεριλαμβάνοντας επίσης στο μήνυμα αυτό ένα διάνυσμα απόστασης με μέγεθος ίσο με τον αριθμό των λογικών υποδικτύων (δηλ, των κόμβων ορόσημων). Μέσω αυτής της διαδικασίας ανταλλαγής, οι καταχωρήσεις στους πίνακες δρομολόγησης με τους μεγαλύτερους αριθμούς ακολουθίας αντικαθιστούν αυτούς με τους μικρότερους.

2.8 Ιεραρχικά Πρωτόκολλα Δρομολόγησης

1)Fisheye State Routing (FSR): Το πρωτόκολλο (FSR) εισάγει την έννοια ενός πολύ-επίπεδου fisheye σχήματος για να μειώσει την συνολική καθυστέρηση της διαδικασίας της δρομολόγησης σε μεγάλα ασύρματα ad-hoc δίκτυα. Οι κόμβοι ανταλλάσσουν τις καταχωρήσεις κατάστασης συνδέσεων με τους γείτονές τους με μια συχνότητα που εξαρτάται από την απόσταση στον προορισμό. Από τις καταχωρήσεις της κατάστασης των συνδέσεων, οι κόμβοι κατασκευάζουν το χάρτη τοπολογίας ολόκληρου του δικτύου και υπολογίζουν τις βέλτιστες διαδρομές. Ο FSR προσπαθεί να βελτιώσει την κλιμάκωση ενός πρωτοκόλλου δρομολόγησης με την προσπάθεια για συγκέντρωση των πληροφοριών της τοπολογίας των κόμβων του δικτύου, που είναι οι πλέον πιθανές να απαιτηθούν για την δρομολόγηση δεδομένων προς αυτούς. Υποθέτει ότι αλλαγές, που στην τοπολογία του τμήματος του δικτύου βρίσκονται κοντύτερα σε έναν κόμβο, είναι πιθανότερο να πρέπει να επεξεργαστούν για την ανανέωση των πληροφοριών δρομολόγησης που κατέχει ο κόμβος αυτός, από ότι οι αλλαγές που συμβαίνουν μακριά από αυτόν. Το πρωτόκολλο φροντίζει να ενημερώνονται συχνότερα, για τις αλλαγές του δικτύου, οι κόμβοι που βρίσκονται κοντύτερα σε αυτές.

2.9 Γεωγραφικά Πρωτόκολλα Δρομολόγησης

1)Location Aided Routing (LAR):Το πρωτόκολλο δρομολόγησης LAR εκμεταλλεύεται τις πληροφορίες θέσεως των κόμβων στο δίκτυο, τις οποίες χρησιμοποιεί για να περιορίσει το πεδίο της πλημμύρας του μηνύματος αναζήτησης μίας νέας διαδρομής, το οποίο υλοποιείται όπως και στα πρωτόκολλα AODV και DSR. Οι πληροφορίες θέσης των κόμβων ενός ad-hoc ασύρματου δικτύου μπορούν να ληφθούν μέσω του GPS (Global Positioning System). Το πρωτόκολλο LAR περιορίζει την αναζήτηση μιας διαδρομής στην αποκαλούμενη ζώνη αιτήματος, που καθορίζεται βασιζόμενη στην

αναμενόμενη θέση του κόμβου προορισμού κατά την διάρκεια της διαδικασίας εύρεσης διαδρομών. Δύο είναι οι σημαντικές σχεδιαστικές αρχές της λειτουργίας του LAR, η αναμενόμενη ζώνη (Expected Zone) και η ζώνη αιτήματος (Request Zone).

Αρχικά θα περιγράψουμε την Αναμενόμενη ζώνη (Expected Zone). Θεωρήστε ότι ένας κόμβος S πρέπει να ανακαλύψει μια διαδρομή προς τον κόμβο D, γνωρίζοντας ότι ο κόμβος D βρισκόταν στη θέση L στο χρόνο t_0 και ότι ο τρέχων χρόνος είναι ti. Η αναμενόμενη ζώνη (Expected Zone) του κόμβου D, από την αντίληψη του κόμβου S στο χρονικό ti είναι η περιοχή που αναμένεται να βρίσκεται ο κόμβος D, την οποία ο κόμβος S μπορεί να καθορίσει γνωρίζοντας την αρχική θέση του κόμβου D, την χρονική στιγμή t_0. Παραδείγματος χάριν, εάν ο κόμβος S γνωρίζει ότι ο κόμβος D ταξιδεύει με μέση ταχύτητα v, μπορεί να υποθέσει ότι η αναμενόμενη ζώνη είναι η κυκλική περιοχή ακτίνας v(t1 - t0), με κέντρο τη θέση L. Εάν η πραγματική ταχύτητα του κόμβου D συμβαίνει να είναι μεγαλύτερη από την μέση, ο κόμβος προορισμού τότε μπορεί να βρίσκεται εκτός από την αναμενόμενη ζώνη την χρονικής στιγμή t_1. Κατά συνέπεια, η αναμενόμενη ζώνη είναι μόνο μια εκτίμηση που γίνεται από τον κόμβο S για να καθορίσει μια περιοχή που ενδεχομένως θα βρίσκεται ο D το χρονικό διάστημα t_1.

Εάν ο κόμβος S δεν γνωρίζει μια προηγούμενη θέση του κόμβου D, δεν μπορεί εύλογα να καθορίσει την αναμενόμενη ζώνη και σε αυτή την περίπτωση ο κόμβος είναι υποχρεωμένος να υποθέσει ότι η ολόκληρη περιοχή που καλύπτεται από το ασύρματο ad-hoc δίκτυο είναι η αναμενόμενη ζώνη). Σε αυτήν την περίπτωση, ο LAR λειτουργεί σαν ένας κλασσικός αλγόριθμος πλημμύρας για την διάδοση των μηνυμάτων αναζήτησης διαδρομών. Γενικά, η γνώση περισσότερων πληροφοριών σχετικά με την κινητικότητα ενός κόμβου οδηγεί στην εύρεση μιας μικρότερης αναμενόμενης ζώνης. Η ζώνη αιτήματος καθορίζεται βάση της αναμενόμενης ζώνης. Θεωρούμε τον κόμβο S που πρέπει να καθορίσει μια διαδρομή προς τον κόμβο D. Ο κόμβος S καθορίζει δυναμικά ή στατικά (implicitly or explicitly) μια ζώνη αιτήματος για την συγκεκριμένη διαδικασία εύρεσης μιας διαδρομής. Ένας κόμβος, που παραλαμβάνει το μήνυμα αυτό, το προωθεί μόνο εάν ανήκει στη ζώνη αιτήματος (σε αντίθεση από τον αλγόριθμό πλημμύρας των AODV και DSR). Για να αυξηθεί η πιθανότητα να φθάσει το αίτημα διαδρομών στον κόμβο D, η ζώνη αιτήματος πρέπει να περιλαμβάνει την αναμενόμενη ζώνη (που περιγράφεται ανωτέρω). Επιπλέον, η ζώνη αιτήματος μπορεί επίσης να περιλάβει και άλλες περιοχές γύρω από τη ζώνη αιτήματος.

Με βάση αυτές τις πληροφορίες ο κόμβος πηγή μπορεί να καθορίσει τις τέσσερις γωνίες της αναμενόμενης ζώνης, τις οποίες συμπεριλαμβάνει στο μήνυμα αιτήματος διαδρομών που μεταδίδει όταν ενεργοποιείται η διαδικασία εύρεσης διαδρομών. Όταν ένας κόμβος λαμβάνει ένα τέτοιο μήνυμα, το απορρίπτει εάν η τωρινή θέση του δεν είναι μέσα στο τμήμα που περιγράφεται από τις συντεταγμένες που περιέχονται στο αίτημα δρομολόγησης.

2) Distance Routing Effect Algorithm for Mobility (DREAM):Ο DREAM είναι ένα πρωτόκολλο δρομολόγησης για τα ad-hoc ασύρματα δίκτυα και βασίζεται σε δύο πρωτότυπες παρατηρήσεις. Η πρώτη, αποκαλούμενη επίδραση στην απόσταση (distance effect), εκμεταλλεύεται το γεγονός ότι όσο μεγαλύτερη η απόσταση που χωρίζει δύο κόμβους, τόσο πιο αργά εμφανίζονται να κινούνται ο ένας σε σχέση με τον άλλο. Συνεπώς οι πληροφορίες θέσης στους πίνακες δρομολόγησης μπορούν να ενημερωθούν συναρτήσει της απόστασης που χωρίζει τους κόμβους χωρίς να γίνεται συμβιβασμός στην ακρίβεια της διαδικασίας της δρομολόγησης. Η δεύτερη ιδέα είναι αυτή που

προκαλεί την αυτόνομη αποστολή πληροφοριών αναπροσαρμογών θέσεως, κινούμενων κόμβων, βασισμένη μόνο στο ποσοστό κινητικότητας κάθε κόμβου. Διαισθητικά είναι σαφές ότι σε έναν κατευθυνόμενο αλγόριθμο δρομολόγησης, για τους πιο αργά κινούμενους κόμβους, πρέπει να ενημερώνουμε λιγότερο συχνά τους πίνακες δρομολόγησης σε σχέση με τους γρηγορότερα κινούμενους κόμβους. Κατ' αυτό τον τρόπο, κάθε κόμβος μπορεί να βελτιστοποιήσει τη συχνότητα με την οποία στέλνει μηνύματα αλλαγών του δικτύου και να μειώνει αντίστοιχα το εύρος ζώνης και την ενέργεια που χρησιμοποιεί, οδηγώντας σε ένα πλήρως κατανεμημένο, αυτόνομο και αποδοτικό σύστημα δρομολόγησης. Με βάση αυτούς τους πίνακες δρομολόγησης, ο προτεινόμενος κατευθυνόμενος αλγόριθμος στέλνει μηνύματα στη "καταγεγραμμένη κατεύθυνση" του κόμβου προορισμού και εγγυάται την παράδοση των δεδομένων προς της κατεύθυνση αυτή με μια δεδομένη πιθανότητα.

2.10 Power Aware Routing Protocol

Σε αυτό το πρωτόκολλο χρησιμοποιούνται μετρήσεις βασισμένες στην ισχύ κατανάλωσης κάθε κόμβου, για την επιλογή των διαδρομών στο ασύρματο ad-hoc δίκτυο. Έχει αποδειχθεί ότι η χρησιμοποίηση τέτοιων χαρακτηριστικών σε έναν αλγόριθμο δρομολόγησης, μειώνει το κόστος ανά πακέτο στην διαδικασία δρομολόγησης κατά 5 - 30 τοις εκατό σε σχέση με τη δρομολόγηση της συντομότερης διαδρομής. Η χρησιμοποίηση τέτοιων μεθόδων εξασφαλίζει ότι ο μέσος χρόνος ζωής των κόμβων αυξάνεται σημαντικά και κατά συνέπειας ο χρόνος που μπορεί το δίκτυο να διατηρηθεί ενεργό αυξάνεται, χωρίς τελικά η καθυστέρηση παράδοσης των δεδομένων να αυξάνεται. Τέτοια πρωτόκολλα έχουν μεγάλη χρήση στην περίπτωση που το ασύρματο ad-hoc δίκτυο αποτελείται από σένσορες, οι οποίοι είναι συσκευές που έχουν περιορισμένη ενέργεια και είναι κρίσιμο να διατηρηθεί το δίκτυο ενεργό όσο το δυνατό περισσότερο.

2.11 Multicast Routing

Το Multicasting είναι η διαδικασία κατά την οποία τα πακέτα δεδομένων από μια συσκευή αποστέλλονται ταυτόχρονα μέσω πολλαπλών μονοπατιών στον προορισμό τους. Όπως και με τα κλασσικά ενσύρματα δίκτυα το multicasting σε ένα MANET είναι επίσης δύσκολο να επιτευχθεί και είναι ακόμα δυσκολότερο στην περίπτωση της κίνησης των κόμβων που δημιουργούν αλλαγή στην τοπολογία του δικτύου αρκετά συχνά. Επομένως, τα πρωτόκολλα δρομολόγησης αυτά, πρέπει να λαμβάνουν υπόψη και τις αλλαγές θέσεως των κόμβων. Αν και δεν είναι τμήμα της συγκεκριμένης εργασίας, θεωρούμε σκόπιμο για λόγους πληρότητας να αναφερθούμε απλά στα δύο σημαντικότερα πρωτόκολλα δρομολόγησης με χρήση πολλαπλών μονοπατιών, το AODV και το ODMRP, που προτείνονται από ομάδα εργασίας MANET της IETF.

1)Multicasting AODV (MAODV):Στον αλγόριθμο δρομολόγησης AODV οι κόμβοι προσχωρούν σε μια ομάδα πολλαπλής προώθησης δεδομένων κατόπιν σχετικής αιτήσεως (on-demand), δημιουργώντας ένα δέντρο πολλαπλής διανομής (multicast-tree) μεταξύ τους. Το δέντρο αυτό αποτελείται από τα μέλη της ομάδας και κόμβους συνδεδεμένους με τα μέλη της ομάδας, επιτρέπει σε έναν άλλο κόμβο να μπορεί να προσχωρήσει σε μια πολλαπλής διανομής ομάδα ακόμα κι αν απαιτούνται περισσότεροι από ένα σύνδεσμοι για να προσεγγίσει ένα άλλο μέλος της ομάδας.

2)On-Demand Multicast Routing Protocol (ODMRP):Το πρωτόκολλο ODMRP βασίζεται στην δημιουργία ενός πλέγματος μεταξύ των κόμβων (mess-based) αντί δέντρου που χρησιμοποιεί το προηγούμενο, που επιτρέπει την δρομολόγηση δεδομένων μέσω πολλαπλών διαδρομών, παρέχοντας καλύτερη συνδεσιμότητα μεταξύ των κόμβων. Με την δημιουργίας ενός πλέγματος παρέχονται πολλαπλές διαδρομές και τα πακέτα μπορούν να παραδοθούν στους προορισμούς τους καθώς οι κόμβοι μετακινούνται και αλλάζουν θέσεις στο δίκτυο. Επιπλέον, τα μειονεκτήματα των multicast δέντρων στα ασύρματα κινητά ad-hoc δίκτυα (π.χ., διαλείπουσα συνδεσιμότητα, συχνός επανα-σχηματισμός του δέντρου, συγκέντρωση κυκλοφορίας, και άλλων) αποφεύγονται. Για να δημιουργηθεί ένα πλέγμα για κάθε ομάδα πολλαπλής διανομής δεδομένων, ο ODMRP χρησιμοποιεί την έννοια της προώθησης ανά ομάδα. Η έννοια αυτή περιγράφει ότι η ομάδα προώθησης (forwarding group) είναι ένα σύνολο αρμόδιων κόμβων για την μετάδοση των multicast δεδομένων. Ο ODMRP ενεργοποιεί τις διαδικασίες δρομολόγησης κατόπιν παραγγελία (on-demand), για να αποφευχθεί η συνολική καθυστέρηση, με στόχο τη βέλτιστη απόδοσης του πρωτοκόλλου σε μεγαλύτερα δίκτυα. Κανένα μήνυμα ελέγχου δεν απαιτείται για να αφήσει ένας κόμβος μια ομάδα.

ΚΕΦΑΛΑΙΟ 3^{Ο}

3.1 Ο Αλγόριθμος Δρομολόγησης Dynamic Source Routing (DSR)

Ο δυναμικός αλγόριθμος δρομολόγησης για ασύρματα ad-hoc δίκτυα είναι ένα απλό και αποδοτικό πρωτόκολλο δρομολόγησης σχεδιασμένο ειδικά για χρήση πάνω από ασύρματα δίκτυα πολλαπλών συνδέσεων (hops) στα οποία οι κόμβοι δεν παραμένουν στάσιμοι αλλά κινούνται. Ο DSR επιτρέπει στο δίκτυο στο οποίο χρησιμοποιείται να είναι πλήρως αυτόνομο, τόσο στην διαδικασία οργάνωσης όσο και στη διαδικασία προσδιορισμού των διαφόρων παραμέτρων του δικτύου, χωρίς να είναι απαραίτητη η παρουσία κάποιας προϋπάρχουσας δικτυακής υποδομής ή διαχείρισης του δικτύου. Το πρωτόκολλο αποτελείται από δύο ξεχωριστούς και αυτόνομους μηχανισμούς, την «Εύρεσης των Διαδρομών» (Route Discovery) και τη «Διατήρησης Διαδρομών» (Route Maintenance), οι οποίες συνεργάζονται και λειτουργούν παράλληλα επιτρέποντας στους κόμβους του δικτύου να ανακαλύπτουν διαδρομές πηγής (source routes) προς κάθε δυνατό προορισμό που επιθυμούν και να τις διατηρούν στην πάροδο του χρόνου λειτουργίας. Η επιλογή της χρήσης διαδρομών πηγής, επιτρέπει την μεταγωγή πακέτων δεδομένων με την χρήση μονοπατιών που δεν περιέχουν βρόγχους. Οι ενδιάμεσοι κόμβοι χωρίς να χρειάζονται επιπλέον πληροφορίες για την κατάσταση των συνδέσεων στο δίκτυο, προωθούν τα πακέτα, σύμφωνα με την διαδρομή που πρέπει να ακολουθήσουν στον επόμενο κόμβο, έως ότου αυτά φτάσουν στον προορισμό του. Παράλληλα οι ενδιάμεσοι κόμβοι αποθηκεύουν σε ειδικούς πίνακες τις πληροφορίες δρομολόγησης, που μεταφέρουν τα πακέτα, για μελλοντική χρήση. Όλες οι λειτουργίες του πρωτοκόλλου λειτουργούν κατόπιν σχετικού αιτήματος από τους ενδιαφερόμενους κόμβους, επιτρέποντας την κλιμάκωση αυτού ανάλογα με τις απαιτήσεις και τις συνθήκες στο δίκτυο.

1) Εισαγωγή: Το δυναμικό πρωτόκολλο δρομολόγησης πηγής (DSR) είναι ένα απλό και αποδοτικό πρωτόκολλο δρομολόγησης που σχεδιάστηκε ειδικά για χρήση σε ασύρματα

ad-hoc δίκτυα πολλαπλών συνδέσεων (hop) κινητών κόμβων. Χρησιμοποιώντας τον DSR, το δίκτυο είναι εντελώς αυτόνομο και δεν απαιτείται η ύπαρξη κάποιας υποδομής ή κεντρικής διαχείρισης αυτού. Οι κόμβοι του δικτύου μπορούν και πρέπει να συνεργάζονται για την μεταφορά των πακέτων από τον ένα στον άλλον, ούτως ώστε να είναι δυνατή η μεταφορά δεδομένων μεταξύ των κόμβων αυτών, που η απευθείας επικοινωνία δεν είναι δυνατή. Καθώς οι κόμβοι στο δίκτυο κινούνται, συνδέονται ή αποσυνδέονται από αυτό, οι συνθήκες του δικτύου, όπως παρεμβολές στο ασύρματο μέσο, εμπόδια στην ασύρματη μετάδοση των δεδομένων και τα δεδομένα δρομολόγησης, καθορίζονται αυτόματα από το πρωτόκολλο δρομολόγησης DSR, δεδομένου ότι ο αριθμός ή η ακολουθία ενδιάμεσων συνδέσεων (hop), που πρέπει να διανύσουν τα πακέτα για να φθάσουν σε οποιοδήποτε πιθανό προορισμό, μπορεί να αλλάξει οποιαδήποτε στιγμή και η προκύπτουσα τοπολογία του δικτύου κάθε στιγμή μπορεί να είναι αρκετά διαφορετική. Το πρωτόκολλο DSR επιτρέπει στους κόμβους να ανακαλύπτουν δυναμικά νέες διαδρομές προς οποιοδήποτε προορισμό του δικτύου. Κάθε πακέτο δεδομένων που αποστέλλεται, μεταφέρει στην επικεφαλίδα (header) του την πλήρη διαδρομή που πρέπει να διανύσει για να φτάσει στον προορισμό του, επιτρέποντας στο πρωτόκολλο δρομολόγησης να είναι λειτουργικό και απλό για τους ενδιάμεσου κόμβους, αποφεύγοντας παράλληλα την ενδεχόμενη ύπαρξη κυκλικών βρόχων μέσα στη διαδρομή. Ταυτόχρονα με την μεταγωγή των πακέτων οι ενδιάμεσοι κόμβοι αποκτούν νέες πληροφορίες δρομολόγησης, τις οποίες τις συλλέγουν και τις αποθηκεύουν σε ειδικούς πίνακες για μελλοντική χρήση.

2) Υποθέσεις στην λειτουργίας του πρωτοκόλλου: Παρακάτω παραθέτουμε μερικές από τις βασικές λειτουργικές υποθέσεις πάνω στις οποίες βασίστηκε η σχεδίαση και η υλοποίηση του πρωτοκόλλου δρομολόγησης DSR.

3) Διαθεσιμότητα των κόμβων και συμμετοχή στις λειτουργίες του πρωτοκόλλου: Υποθέτουμε ότι όλοι οι κόμβοι του δικτύου, που επιθυμούν να επικοινωνήσουν με άλλους κόμβους μέσα σε ένα ad-hoc δίκτυο, είναι πρόθυμοι να συμμετέχουν πλήρως στην διαδικασία δρομολόγησης των πακέτων του δικτύου. Συγκεκριμένα, κάθε κόμβος που συμμετέχει στο δίκτυο, πρέπει να είναι πρόθυμος να μεταγάγει πακέτα για τους άλλους κόμβους του δικτύου.

4) Διάμετρος του δικτύου: Αναφερόμαστε στον ελάχιστο αριθμό μονοπατιών που απαιτούνται, για να μεταδοθεί ένα πακέτο, από οποιοδήποτε κόμβο που βρίσκεται σε μία ακριανή θέση του ad-hoc δικτύου, σε έναν άλλο κόμβο που βρίσκεται στο αντίθετο άκρο, σαν «διάμετρο» του δικτύου. Υποθέτουμε ότι η διάμετρος ενός τέτοιου δικτύου θα είναι συχνά μικρή (π.χ. με τιμές από 5 έως 10 μονοπάτια).

5) Αλλοιωμένα πακέτα: Τα πακέτα που μεταδίδονται σε ένα ασύρματο δίκτυο μπορεί να χαθούν ή να αλλοιωθούν. Ένας κόμβος που λαμβάνει ένα αλλοιωμένο πακέτο έχει την ικανότητα να το ανιχνεύσει και να το απορρίψει.

6) Μοντέλο κίνησης των κόμβων: Οι κόμβοι μέσα στο ειδικό δίκτυο μπορούν να κινηθούν οποιαδήποτε στιγμή χωρίς προειδοποίηση και να συνεχίσουν να κινούνται συνεχώς και προς τυχαία κατεύθυνση. Υποθέτουμε ότι η ταχύτητα με την οποία οι κόμβοι κινούνται είναι συγκρίσιμη (moderate) σε σχέση με την καθυστέρηση στην ασύρματη μετάδοση των πακέτων από τα χαμηλότερα επίπεδα του δικτύου. Συγκεκριμένα ο DSR μπορεί να υποστηρίξει δίκτυα στα οποία οι κόμβοι τους κινούνται με οποιαδήποτε ταχύτητα, αργά ή γρήγορα, και προς οποιαδήποτε τυχαία κατεύθυνση. Υποθέτουμε όμως ότι οι κόμβοι δεν κινούνται συνεχώς τόσο γρήγορα ώστε να αναγκάζουν το πρωτόκολλο να ενεργοποιεί για κάθε πακέτο την διαδικασία εύρεσης

μίας νέας διαδρομής, με αποτέλεσμα η καθυστέρηση στη μετάδοση να είναι πολύ μεγαλύτερη από την περίπτωση χρήσης της τεχνικής της πλημμύρα κάθε μεμονωμένου πακέτου στο δίκτυο, ελπίζοντας κάποιο από αυτά να φτάσει στον προορισμό του.

7) Λειτουργία promiscuous mode: Υποθέτουμε ότι οι κόμβοι μπορούν να ενεργοποιήσουν την λειτουργία promiscuous mode στο υλικό της ασύρματης διεπαφής του δικτύου τους, αναγκάζοντας το να παραδίδει κάθε λαμβανόμενο πακέτο στα ανώτερα στρώματα του δικτύου, χωρίς να φιλτράρει τη διεύθυνση προορισμού των πακέτων, απορρίπτοντας όλα αυτά που δεν προορίζονται για τον συγκεκριμένο κόμβο. Με αυτόν τον τρόπο οι κόμβοι λαμβάνουν όλα τα πακέτα που μπορούν να «ακούσουν» στο ασύρματο κανάλι. Αν και δεν απαιτείται, η δυνατότητα αυτή είναι κοινή στο υλικό που χρησιμοποιείται στις δικτυακές ασύρματες κάρτες σήμερα και μερικές από τις βελτιστοποιήσεις του πρωτοκόλλου DSR μπορούν να εκμεταλλευθούν τη δυνατότητα αυτή. Η χρήση του promiscuous τρόπου μπορεί επίσης να αυξάνει την κατανάλωση ισχύς του υλικού του δικτύου, αφού πρέπει ο ασύρματος πομποδέκτης να μένει ενεργός πολύ περισσότερο χρόνο. Αν και έχει παρατηρηθεί ότι οι βελτιστοποιήσεις που έχουν γίνει κάνουν τον DSR περισσότερο αποδοτικό, το πρωτόκολλο μπορεί εύκολα να χρησιμοποιηθεί και χωρίς αυτές ή να προγραμματιστεί, ώστε να τις ενεργοποιεί περιοδικά.

8)Αμφίδρομη και μη-αμφίδρομη επικοινωνία: Η δυνατότητα ασύρματης επικοινωνίας μεταξύ οποιωνδήποτε κόμβων μπορεί κατά περιόδους να μην λειτουργεί εξίσου καλά και προς στις δύο κατευθύνσεις, οφειλόμενη παραδείγματος χάριν, στην χρήση διαφορετικών κεραιών σε κάθε κόμβο, παν-κατευθυντικών ή κατευθυντικών, διάδοσης των ηλεκτρομαγνητικών κυμάτων ή των πηγών παρεμβολών γύρω από τους κόμβους. Αυτό έχει σαν αποτέλεσμα η επικοινωνία μεταξύ δυο κόμβων σε πολλές περιπτώσεις να λειτουργεί και προς τις δύο κατευθύνσεις, αλλά σε άλλες να λειτουργεί μόνο προς τη μία κατεύθυνση, κάθε χρονική στιγμή, επιτρέποντας την επικοινωνία προς την μία φορά. Αν και πολλά πρωτόκολλα δρομολόγησης λειτουργούν σωστά μόνο στην πρώτη περίπτωση ο DSR μπορεί επιτυχώς να ανακαλύψει τις διαδρομές σε ένα δίκτυο και να δρομολογήσει τα πακέτα τόσο στην πρώτη όσο και στην δεύτερη περίπτωση. Αν και μερικά πρωτόκολλα περιορίζονται να χρησιμοποιούνται στην περίπτωση που χρησιμοποιείται ο ένας ή ο άλλος τύπος από συνδέσεις, ο DSR μπορεί να λειτουργήσει εξίσου καλά και αποδοτικά και με τα δύο, εκμεταλλευόμενος πρόσθετες βελτιστοποιήσεις.

9) Ανάθεση διευθύνσεων IP στους κόμβους του δικτύου: Κάθε κόμβος επιλέγει μια μοναδική διεύθυνση IP από την οποία αναγνωρίζεται στο δίκτυο. Αν και ένας κόμβος μπορεί να έχει πολλές διαφορετικές διεπαφές δικτύων και όπως σε ένα κλασικό δίκτυο IP, σε κάθε μια από αυτές θα αντιστοιχούσε μια διαφορετική διεύθυνση IP, απαιτούμε από τους κόμβους, κατά την συμμετοχή στο πρωτόκολλο DSR, να επιλέξουν και να χρησιμοποιούν μόνο μία από τις διευθύνσεις αυτές. Με τον τρόπο αυτό κάθε κόμβος μπορεί να αναγνωριστεί από όλους τους υπόλοιπους στο δίκτυο, ανεξάρτητα από το ποια συγκεκριμένη διεπαφή χρησιμοποιείται. Σύμφωνα με την ορολογία που χρησιμοποιείται από το Mobile IP, αναφερόμαστε στη διεύθυνση την οποία χρησιμοποιεί κάθε κινητός κόμβος σε ένα ad-hoc δίκτυο ως «home address». Η διεύθυνση αυτή μπορεί να οριστεί από οποιοδήποτε μηχανισμό (στατική ή δυναμική ανάθεση, με χρήση DHCP). Η επιλογή της μεθόδου ανάθεσης διευθύνσεων IP είναι έξω από το πεδίο και το σκοπό του πρωτοκόλλου δρομολόγησης DSR και δεν επηρεάζει την απόδοση του.

3.2 Περιγραφή του πρωτοκόλλου DSR

1) Επισκόπηση και Σημαντικές Ιδιότητες του πρωτοκόλλου: Το πρωτόκολλο δρομολόγησης DSR αποτελείται από δύο μηχανισμούς που λειτουργούν (συνεργάζονται) ταυτόχρονα για την ανακάλυψη διαδρομών και τη διατήρηση τους σε ένα ασύρματο ad-hoc τηλεπικοινωνιακό δίκτυο.

Η εύρεση διαδρομών είναι ο μηχανισμός κατά τον οποίο ένας κόμβος S που επιθυμεί να στείλει ένα πακέτο σε έναν κόμβο προορισμού D ζητάει και λαμβάνει μια διαδρομή για τον κόμβο αυτό. Ο μηχανισμός αυτός χρησιμοποιείται μόνο όταν επιχειρεί ο κόμβος S να στείλει ένα πακέτο στον D και δεν γνωρίζει ήδη μια διαδρομή προς αυτόν.

Η συντήρηση διαδρομών είναι ο μηχανισμός κατά τον οποίο ένας κόμβος S ανιχνεύει, αν μια ήδη υπάρχουσα και χρησιμοποιούμενη διαδρομή για έναν κόμβο προορισμού D είναι σωστή ή όχι επιτρέποντας την επικοινωνία ανάμεσα τους, στην περίπτωση που η τοπολογία του δικτύου έχει αλλάξει και δεν είναι δυνατόν να χρησιμοποιηθεί η διαδρομή αυτή, επειδή κατά μήκος της διαδρομής ένα μονοπάτι δεν λειτουργεί. Όταν η διαδικασία αυτή υποδείξει μια διαδρομή η οποία σε κάποιο σημείο είναι «διακομμένη», δηλαδή μία συγκεκριμένη σύνδεση μεταξύ δύο κόμβων της διαδρομής έχει διακοπεί, ο κόμβος S μπορεί να προσπαθήσει να χρησιμοποιήσει οποιαδήποτε άλλη διαδρομή συμβαίνει να γνωρίζει για τον D ή να ενεργοποιήσει την διαδικασία εύρεσης διαδρομών για τον D. Η συντήρηση διαδρομών χρησιμοποιείται μόνο κατά την διάρκεια αποστολής δεδομένων από τον S στον D. Η εύρεση και η συντήρηση διαδρομών λειτουργούν εξ ολοκλήρου αυτόνομα και μόνο μετά από αντίστοιχη αίτηση ενός κόμβου. Ειδικότερα και αντίθετα από άλλα πρωτόκολλα, ο DSR δεν απαιτεί την ύπαρξη περιοδικά λαμβανόμενων μηνυμάτων ελέγχου, με πληροφορίες για τις αλλαγές στις διαδρομές του δικτύου, λόγω της αλλαγής της φυσικής θέσης των κόμβων, για την συντήρηση των διαδρομών που έχουν ήδη ανακαλυφθεί. Και οι δυο βασικοί μηχανισμοί λειτουργίας του πρωτοκόλλου ενεργοποιούνται μόνο μετά από σχετική απαίτηση των κόμβων του δικτύου, επιτρέποντας έτσι την κλιμάκωση της κίνησης που δημιουργούν τα πακέτα ελέγχου του DSR, για την εύρεση και συντήρηση των διαδρόμων προς το μηδέν, όταν όλοι οι κόμβοι είναι περίπου στάσιμοι και όλες οι διαδρομές που απαιτούνται για την τρέχουσα επικοινωνία έχουν ήδη ανακαλυφθεί. Αυτό σημαίνει ότι η κίνηση που δημιουργείται λόγω των πακέτων των διαδικασιών εύρεσης και συντήρησης διαδρομών κλιμακώνεται ανάλογα και προσαρμόζεται σύμφωνα με τις ανάγκες του πρωτοκόλλου για την επιτυχή δρομολόγηση των πακέτων δεδομένων, ανάλογα με την κινητικότητα και σχετική θέση των κόμβων στο δίκτυο, (δηλ. αυξάνεται όταν παρατηρείται μεγάλη κινητικότητα και μειώνεται όταν η κινητικότητα είναι μικρή). Οι κόμβοι συνήθως αποθηκεύουν μόνο μία διαδρομή για κάθε προορισμό μέσα σε ένα ad-hoc δίκτυο, είτε αυτή προκύπτει από την διαδικασία εύρεσης διαδρομών, είτε από τις πληροφορίες δρομολόγησης, που συλλέγουν κατά την μεταγωγή πακέτων δεδομένων. Ένας κόμβος όμως μπορεί να αποθηκεύσει πολλαπλές διαδρομές για οποιοδήποτε προορισμό. Αυτό επιτρέπει την γρήγορη αντίδραση των πρωτοκόλλων δρομολόγησης, εξαιτίας των αλλαγών των τοπολογικών χαρακτηριστικών του δικτύου, οι οποίες έχουν σαν άμεσο αποτέλεσμα την ανάγκη εύρεσης νέων διαδρομών προς τους προορισμούς. Σε μία τέτοια περίπτωση ο κόμβος μπορεί να χρησιμοποιήσει μία από τις αποθηκευμένες διαδρομές προς τον προορισμό, όταν αυτή που ήδη χρησιμοποιεί αποτύχει στην αποστολή των δεδομένων. Ο μηχανισμός αυτός δημιουργεί μικρότερη καθυστέρηση στην εύρεση μιας νέας διαδρομής, μετά από την ανακάλυψη μιας «διακομμένης» διαδρομής, από την καθυστέρηση που θα παρατηρούσαμε από την ενεργοποίηση ξανά της διαδικασίας εύρεσης διαδρομών.

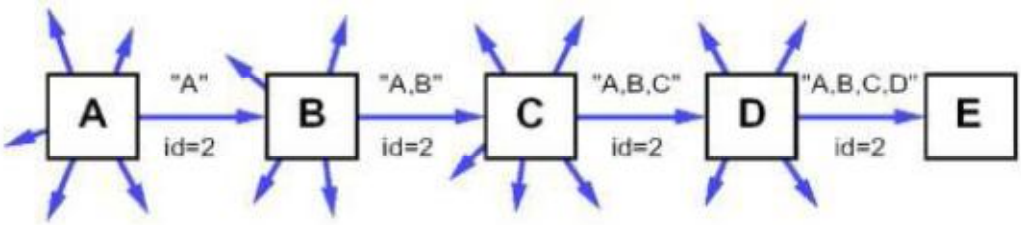
Η λειτουργία της εύρεσης και της συντήρηση διαδρομών υποστηρίζονται, τόσο από ασύρματα κανάλια που λειτουργούν είτε προς την μία ή την άλλη κατεύθυνση, όσο και από κανάλια που υποστηρίζουν την μετάδοση δεδομένων ταυτόχρονα και προς τις δύο κατευθύνσεις. Ο DSR επιτρέπει σε ένα ασύρματο ad-hoc δίκτυο την ύπαρξη και των δύο τύπων ασύρματων καναλιών αφού μπορεί να λειτουργήσει εξίσου αποδοτικά και στις δύο περιπτώσεις.

Τελειώνοντας την επισκόπηση των σημαντικότερων χαρακτηριστικών του DSR αναφέρουμε ότι υποστηρίζει επίσης και τη δια-σύνδεση ενός ασύρματου ad-hoc δικτύου με ένα οποιοδήποτε άλλο δίκτυο, διαφορετικού τύπου, επιτρέποντας σε μια διαδρομή από την πηγή προς τον κόμβο προορισμού, να μπορεί να αποτελείται από μονοπάτια κόμβων που ανήκουν είτε στο ένα είτε στο άλλο δίκτυο. Υποστηρίζει την εύρεση διαδρομών για κόμβους που βρίσκονται έξω από ένα ad-hoc δίκτυο και ανήκουν στον παγκόσμιο δικτυακό ιστό, αρκεί ο κόμβος του ad-hoc δικτύου που χρησιμοποιείται ως «πύλη» (gateway) να μπορεί να συμπληρώσει την αίτηση για το εν λόγω μονοπάτι και να επιστρέψει την πλήρη διαδρομή στην πηγή, με το κομμάτι που ανήκει στο άλλο δίκτυο. Στην περίπτωση αυτή ο κόμβος που ανήκει και στα δύο δίκτυα ονομάζεται «κόμβος πύλη» (gateway) και μπορεί να χρησιμοποιεί αλγόριθμους δρομολόγησης διαφορετικούς από τον DSR.

3.3 Μηχανισμός εύρεσης διαδρομών

Όταν κάποιος κόμβος S δημιουργεί ένα νέο πακέτο που προορίζεται για κάποιον άλλο κόμβο D, τοποθετεί στην επικεφαλίδα του πακέτου αυτού μια διαδρομή πηγής που δίνει την ακολουθία των κόμβων και συνδέσεων (hops), που το πακέτο πρέπει να ακολουθήσει για να φτάσει στον προορισμό του. Σύμφωνα με το πρωτόκολλο DSR, ο κόμβος S θα αποκτήσει μια κατάλληλη διαδρομή δρομολόγησης από την cache, μια ειδική μνήμη που έχει αποθηκευμένες τις διαδρομές προς τους διάφορους κόμβους του ad-hoc δικτύου, που έχει ανακαλύψει μέχρι την παρούσα χρονική στιγμή. Εάν όμως κάποια διαδρομή δεν βρίσκεται στην cache, το πρωτόκολλο θα ενεργοποιήσει τον μηχανισμό εύρεσης διαδρομών για να βρει μια νέα διαδρομή προς τον S. Σε αυτήν την περίπτωση καλούμε τον S κόμβο προέλευσης και τον D κόμβο προορισμού του μηχανισμού εύρεσης διαδρομών.

Στην παρακάτω εικόνα περιγράφεται ένα παράδειγμα εύρεσης μιας διαδρομής, στο οποίο ένας κόμβος A προσπαθεί να ανακαλύψει μια διαδρομή προς τον κόμβο E. Για να ξεκινήσει η διαδικασία, ο κόμβος A μεταδίδει ένα μήνυμα «Route Request» προς όλους τους κόμβους οι οποίοι βρίσκονται στην εμβέλεια του. Κάθε τέτοιο μήνυμα προσδιορίζει τους κόμβους προέλευσης και προορισμού και περιέχει ένα αριθμό μοναδικό και καθορισμένο από τον κόμβο προέλευσης του κάθε αιτήματος εύρεσης μιας διαδρομής. Κάθε τέτοιο μήνυμα επίσης περιέχει ένα πεδίο στο οποίο υπάρχουν οι διευθύνσεις κάθε ενδιάμεσου κόμβου μέσω του οποίου τα αντίγραφο του αρχικού αιτήματος έχουν διαβιβαστεί και καταλήξει στον κόμβο αυτό. Αυτό το πεδίο αρχικοποιείται με έναν κενό κατάλογο όταν ενεργοποιείται η διαδικασία εύρεσης διαδρομών.



Εικόνα 11. *Μηχανισμός Εύρεσης Διαδρομών*

Όταν ένας κόμβος λαμβάνει ένα «Route Request», εάν είναι ο κόμβος προορισμού της συγκεκριμένης διαδικασία εύρεσης διαδρομής, επιστρέφει ένα μήνυμα «Route Reply» στον κόμβο προέλευσης του αιτήματος, δίνοντας και ένα αντίγραφο του πεδίου των διαδρομών από το πακέτο του «Route Request». Όταν ο κόμβος προέλευσης λάβει το «Route Reply», αποθηκεύει στην «Route Cache» του την διαδρομή, για τη χρήση της στην μετέπειτα αποστολή των δεδομένων. Εάν ο κόμβος που λαμβάνει το «Route Request» έχει δει πρόσφατα και άλλο μήνυμα «Route Request» από τον ίδιο προορισμό με τον ίδιο αριθμό ταυτότητας στο αίτημα ή εάν διαπιστώνει ότι η διεύθυνσή του κόμβου αυτού παρατίθεται ήδη στο πεδίο διαδρομών του μηνύματος, αγνοεί το συγκεκριμένο μήνυμα και καταστρέφει το σχετικό πακέτο. Διαφορετικά, αυτός ο κόμβος επισυνάπτει τη διεύθυνσή του στο πεδίο διαδρομών στο μήνυμα «Route Request» και το προωθεί σε όλους τους κόμβους που βρίσκονται στην εμβέλεια του, με τον ίδιο αριθμό ταυτότητας του συγκεκριμένου αιτήματος, για να συνεχιστεί η διαδικασία.

Στην επιστροφή του μηνύματος «Route Reply» από τον κόμβος Ε, στον κόμβο Α που ενεργοποίησε την διαδικασία, βλέπε στο παραπάνω σχήμα, θα προσπαθήσει να εντοπίσει και ο Ε μία διαδρομή προς τον Α, χρησιμοποιώντας αρχικά την «Route Cache» για να εντοπίσει την διαδρομή αυτή. Εάν βρίσκεται εκεί μια διαδρομή θα τη χρησιμοποιήσει, ενώ σε διαφορετική περίπτωση θα ενεργοποιήσει τον μηχανισμό εύρεσης διαδρομών. Για να αποφύγουν πιθανές άπειρες επαναλήψεις της διαδικασίας αυτής, δηλαδή των επαναλαμβανόμενων διαδικασιών εύρεσης διαδρομών, ο κόμβος Ε πρέπει να μεταφέρει στο μήνυμα της αίτησης για την διαδρομή προς τον Α «Route Request» και την απάντηση του, «Route Reply», στην πρότερη αίτηση από τον Α. Ο κόμβος Ε θα μπορούσε απλά να αντιστρέψει την ακολουθία των μονοπατιών, που υπάρχει στο πεδίο διαδρομών, της αίτησης για εύρεση της διαδρομής που έλαβε και να χρησιμοποιήσει αυτή την διαδρομή για να αποστείλει την απάντηση του στον κόμβο προέλευσης του αιτήματος, μόνο αν το πρωτόκολλο MAC, όπως αυτό του IEEE 802.11, υποστηρίζει κανάλια που επιτρέπουν την ταυτόχρονη αποστολή δεδομένων και προς τις δύο κατευθύνσεις, (δηλ μία ενεργή σύνδεση από ένα κόμβο Α στον Β, προϋποθέτει, εξαιτίας του πρωτοκόλλου MAC, ότι και η σύνδεση από τον Β στον Α είναι ενεργή). Εντούτοις στον DSR υποστηρίζονται συνδέσεις που επιτρέπουν την μεταφορά δεδομένων είτε προς την μία είτε προς την άλλη κατεύθυνση είτε και προς τις δύο, οπότε ο μηχανισμός εύρεσης των διαδρομών είναι σχεδιασμένος για να υποστηρίζει και τους δύο τύπους καναλιών επικοινωνίας.

Κατά την έναρξη του μηχανισμού ανακάλυψης διαδρομών, ο κόμβος προέλευσης του αιτήματος αποθηκεύει ένα αντίγραφο του αρχικού μηνύματος σε έναν τοπικό προσωρινό πίνακα που ονομάζεται «Send Buffer» . Ο πίνακας αυτός περιέχει ένα αντίγραφο κάθε πακέτου, που δεν μπορεί να διαβιβαστεί από τον συγκεκριμένο κόμβο, επειδή δεν υπάρχει διαθέσιμη ακόμα μια διαδρομή πηγής προς τον προορισμό του πακέτου. Κάθε τέτοιο πακέτο είναι μαρκαρισμένο με την χρονική στιγμή που τοποθετήθηκε στον «Send

Buffer». Κάθε πακέτο είναι προβλεπόμενο να διαγραφεί από τον πίνακα αυτό μετά από κάποια προϋπολογισμένη περίοδο. Εάν είναι απαραίτητο να αντικαταστήσουμε κάποια εγγραφή λόγω υπέρ-πληρότητας, χρησιμοποιούμε κάποιο αλγόριθμο αντικατάστασης δεδομένων, όπως ο (First In First Out, FIFO) ή οποιοδήποτε άλλο.

Όσο ένα πακέτο παραμένει στον «Send Buffer», ο κόμβος πρέπει περιστασιακά να φροντίσει να ενεργοποιεί ξανά τον μηχανισμό εύρεσης διαδρομών για τον προορισμό του πακέτου και ανάλογα με την πάροδο του χρόνου πρέπει να φροντίζει να μειώνει την συχνότητα ενεργοποίησης αυτής της διαδικασίας. Όταν για ένα προορισμό δεν καταφέρνουμε, για ένα μεγάλο χρονικό διάστημα, να βρούμε μία διαδρομή είναι πιθανό ο κόμβος αυτός να είναι εκτός του δικτύου και να μην είναι δυνατό να βρούμε τελικά μια τέτοια διαδρομή. Συγκεκριμένα, λόγω της περιορισμένης ασύρματης εμβέλειας των κόμβων και της κίνησης τους μέσα στο δίκτυο, κατά περιόδους το δίκτυο μπορεί να κατατμηθεί σε δύο ή περισσότερα τμήματα με αποτέλεσμα να μην υπάρχει την δεδομένη χρονική περίοδο καμία ακολουθία μονοπατιών μεταξύ των κόμβων, μέσω των οποίων ένα πακέτο θα μπορούσε να διαβιβαστεί για να φθάσει στον προορισμό του. Ανάλογα με το μοντέλο μετακίνησης των κόμβων και την πυκνότητα των κόμβων στο δίκτυο, τέτοιες κατατμήσεις στα ad-hoc δικτύων μπορούν να είναι σπάνιες ή μπορεί να συμβαίνουν συχνά.

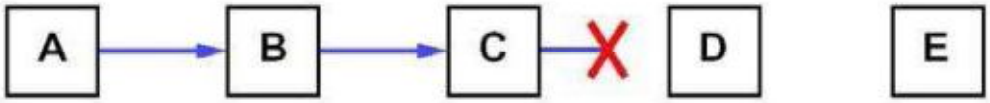
Εάν για κάθε μια τέτοια κατάσταση ενεργοποιείται ο μηχανισμός εύρεσης διαδρομών για κάθε πακέτο, ένας πολύ μεγάλος αριθμός από μη παραγωγικά «Route requests» θα προωθούνταν σε άλλους κόμβους του δικτύου. Για την μείωση του φαινομένου αυτού χρησιμοποιούμε μια τεχνική που ονομάζεται «exponential back-off», για να περιοριστεί ο ρυθμός με τον οποίο ενεργοποιούνται οι νέες ανακαλύψεις διαδρομών από οποιοδήποτε κόμβο του δικτύου, πάντα προς τον ίδιο κόμβο προορισμού. Εάν ένας κόμβος προσπαθεί να αποστείλει πακέτα δεδομένων προς τον ίδιο κόμβο συχνότερα από ότι το σχετικό όριο επιτρέπει, τα πακέτα που δεν μπορούν να μεταδοθούν πρέπει να αποθηκευτούν στον «Send Buffer», έως ότου παραλάβει ο κόμβος αυτός ένα «Route Reply», αλλά και πάλι ο κόμβος πρέπει να μην ενεργοποιεί την αναζήτηση διαδρομών μέχρι το ελάχιστο επιτρεπόμενο όριο για τον συγκεκριμένο προορισμό επιτευχθεί.

3.4 Μηχανισμός συντήρησης διαδρομών στον DSR

Ο κόμβος που δημιουργεί ή προωθεί ένα πακέτο χρησιμοποιώντας μια διαδρομή πηγής, είναι αρμόδιος για την λήψη της επιβεβαίωσης, ότι το πακέτο έχει παραληφθεί επιτυχώς από τον επόμενο στη διαδρομή δρομολόγησης κόμβο. Το πακέτο αυτό μπορεί να μεταδοθεί ξανά μέχρι έναν μέγιστο αριθμό προσπαθειών έως ότου η επιβεβαίωση για την επιτυχή μετάδοση του παραληφθεί.

Στο παράδειγμα που περιγράφεται στο παρακάτω σχήμα, ο κόμβος A έχει δημιουργήσει ένα πακέτο για να το μεταδώσει στον κόμβο E, χρησιμοποιώντας μια διαδρομή πηγής, μέσω των ενδιάμεσων κόμβων B, C, και D. Σε αυτήν την περίπτωση, ο κόμβος A είναι αρμόδιος για την λήψη του πακέτου από τον B, ο κόμβος B είναι αρμόδιος για την λήψη από τον C, ο κόμβος C είναι αρμόδιος για την λήψη από τον D, και ο κόμβος D είναι αρμόδιος για την παραλαβή του πακέτου τελικά από τον προορισμό E. Οι επιβεβαιώσεις παραλαβής των πακέτων από τον ένα κόμβο στον άλλο πάνω στο μονοπάτι της διαδρομής, σε πολλές περιπτώσεις, προσφέρονται στο πρωτόκολλο DSR χωρίς κόστος, είτε λόγω του υπάρχοντος πρωτοκόλλου MAC που χρησιμοποιείται (όπως οι επιβεβαιώσεις που υποστηρίζονται, στο επίπεδο συνδέσεων του δικτύου, από το πρότυπο της IEEE 802.11), είτε από τις λεγόμενες παθητικές επιβεβαιώσεις (passive

acknowledgements), στις οποίες ένας κόμβος επιβεβαιώνει μια επιτυχημένη παραλαβή από έναν άλλο κόμβο, προσπαθώντας να ακούσει τον άλλο κόμβο να μεταδίδει το πακέτο που έλαβε επιτυχώς, με τη σειρά του, στον επόμενο κόμβο. Εάν κανένας από αυτούς τους μηχανισμούς επιβεβαίωσης δεν είναι διαθέσιμος, ο κόμβος που διαβιβάζει το πακέτο μπορεί να θέσει ένα ειδικό πεδίο, στην επικεφαλίδα του πακέτου (header), για να ζητήσει την αποστολή μιας επιβεβαίωσης από το πρωτόκολλο δρομολόγησης. Το πρόβλημα σε αυτή την περίπτωση είναι ότι εφόσον θα αναλάβει ο DSR να στείλει το μήνυμα επιβεβαίωσης, θα το κάνει χρησιμοποιώντας τις μεθόδους της μετάδοσης πακέτων δεδομένων, δηλαδή είτε θα χρησιμοποιήσει την σύνδεση ανάμεσα στους δύο κόμβους, εάν αυτή υποστηρίζει την μετάδοση δεδομένων και προς τις δύο κατευθύνσεις, ή στην περίπτωση που αυτό δεν συμβαίνει θα προσπαθήσει να εντοπίσει μια διαδρομή προς τον κόμβο αυτό, το οποίο μπορεί να έχει σαν αποτέλεσμα το μήνυμα επιβεβαίωσης να ταξιδέψει από διαφορετικό μονοπάτι.



Εικόνα 12. *Περίπτωση ενεργοποίησης μηχανισμού συντήρησης διαδρομών*

Εάν ένας κόμβος έχει να προωθήσει ένα πακέτο το οποίο έχει ξεπεράσει το μέγιστο αριθμό αναμεταδόσεων, χωρίς να έχει λάβει επιβεβαίωση για την παραλαβή του, αυτός ο κόμβος δημιουργεί ένα μήνυμα «Route Error» και το στέλνει στον κόμβο που είχε αρχικά δημιουργήσει το πακέτο αυτό. Μέσα σε αυτό το μήνυμα περιέχονται όλες οι πληροφορίες για την σύνδεση πέρα από την οποία το πακέτο δεν μπορούσε να μεταδοθεί. Στην παραπάνω εικόνα, εάν ο κόμβος C δεν καταφέρει να παραδώσει το πακέτο που θέλει να προωθήσει στον επόμενο κόμβο D, επιστρέφει ένα μήνυμα «Route Error» στον κόμβο A, δηλώνοντας ότι η σύνδεση από τον C στον D είναι «διακομμένη». Ο κόμβος A αφαιρεί στη συνέχεια αυτήν την διαδρομή από την «Route Cache», θεωρώντας την άκυρη και οποιαδήποτε αναμετάδοση του αρχικού πακέτου στον προορισμό του είναι μια λειτουργία που θα εκτελέσουν τα ανώτερα στρώματα του δικτύου όπως το TCP, όταν το αντιληφθούν. Ο κόμβος A στην συνέχεια μπορεί να χρειαστεί μία νέα διαδρομή προς τον κόμβο E και για το λόγο αυτό πρέπει να μπορέσει να αντικαταστήσει την συγκεκριμένη διαδρομή με μία καινούρια ενεργή. Οι επιλογές που έχει είναι να χρησιμοποιήσει μία διαδρομή που βρίσκεται στην «Route Cache» του ή να ενεργοποιήσει τον μηχανισμό εύρεσης διαδρομών για τον συγκεκριμένο κόμβο, για να ανακαλύψει μια νέα διαδρομή, για να στείλει τελικά τα πακέτα δεδομένων.

ΚΕΦΑΛΑΙΟ 4^{Ο}

4.1 Ο Αλγόριθμος Δρομολόγησης Ad - hoc On Demand Distance Vector (AODV)

1) Εισαγωγή: Λόγω του γεγονότος της απουσίας συσκευών δρομολόγησης σε ένα ad - hoc δίκτυο, κάθε κόμβος θα πρέπει να συνεισφέρει στην δρομολόγηση, στην ασφάλεια

και γενικότερα στη ομαλή λειτουργία του δικτύου. Λόγω της απουσίας «κεντρικού ελέγχου» γίνεται πολύ ευκολότερη η διείσδυση μη εξουσιοδοτημένων μονάδων στο δίκτυο. Με άλλα λόγια οι κίνδυνοι ασφαλείας είναι πολύ μεγαλύτεροι. Επίσης η συνεχής κίνηση των κόμβων αλλά και το γεγονός χρήσης ασύρματου και όχι ενσύρματου διαύλου, συμβάλουν με τον τρόπο τους στην ανάγκη για έμφαση στην ασφάλεια αυτού του είδους των δικτύων. Αυτό αλλά και άλλα χαρακτηριστικά των ad - hoc δικτύων, κάνουν τη δρομολόγηση ένα αρκετά ενδιαφέρον πεδίο για τους ερευνητές. Ο ad - hoc On - Demand Distance Vector είναι ένας από τους ευρύτερα χρησιμοποιούμενους αλγορίθμους, αλλά και ένας αλγόριθμος που συνεχώς εξελίσσετε και συμπληρώνετε με το πέρασμα του χρόνου, κυρίως στο κομμάτι της ασφάλειας.

2) Ασφάλεια Επικοινωνίας: Σε γενικές γραμμές, δύο είναι οι πιθανές επιθέσεις σε ένα ad - hoc δίκτυο:

- Παθητικές (passive) και
- Ενεργητικές (active)

Στην πρώτη κατηγορία, ο επιτιθέμενος δεν παρεμβαίνει στο πρωτόκολλο δρομολόγησης. Αυτό που κάνει είναι να παρακολουθεί και να καταγράφει της κίνηση προσπαθώντας με τον τρόπο αυτό να εξάγει χρήσιμες γι' αυτόν πληροφορίες σχετικά με την ιεραρχία των κόμβων, την τοπολογία του δικτύου κ.τ.λ.

Στην δεύτερη κατηγορία (active attacks), οι «επιτιθέμενοι» κόμβοι, παρεμβαίνουν στην ομαλή λειτουργία του πρωτοκόλλου, μεταβάλλοντας τις πληροφορίες δρομολόγησης, παρέχοντας εσφαλμένες πληροφορίες αλλά και προσποιούμενοι άλλους «πιστοποιημένους» κόμβους.

Σε γενικές γραμμές, κρυπτογραφικοί μηχανισμοί χρησιμοποιούνται για την προστασία των πρωτοκόλλων δρομολόγησης, με την εφαρμογή αμοιβαίων σχέσεων εμπιστοσύνης μεταξύ των κόμβων. Το πρόβλημα της ασφάλειας είναι και το βασικό πρόβλημα στα ad - hoc δίκτυα και μπορεί να χωριστεί σε δύο κατηγορίες.

- Η πρώτη κατηγορία έχει να κάνει με την ασφάλεια τις επικοινωνίας των κόμβων μεταξύ τους και
- Η δεύτερη με την ασφάλεια των δεδομένων που μεταφέρονται στο ασύρματο μέσο.

Στο κεφάλαιο αυτό θα εξετάσουμε το κλασικό πρωτόκολλο δρομολόγησης AODV αλλά και τα μειονεκτήματα ασφαλείας που αυτό περιέχει. Στη συνέχεια θα μελετήσουμε τις προτάσεις που έγιναν από διάφορους ερευνητές προς την κατεύθυνση της αύξησης του επιπέδου ασφαλείας για το πρωτόκολλο αυτό.

3) Περιγραφή του Πρωτοκόλλου AODV: Το πρωτόκολλο AODV δεν έχει ανάγκη κανενός κεντρικού συστήματος διαχείρισης για τον έλεγχο της διαδικασίας δρομολόγησης. Τα reactive πρωτόκολλα όπως το AODV τείνουν αν ελαττώνουν το φόρτο λόγω των μηνυμάτων ελέγχου κίνησης (control traffic messages) πληρώνοντας το κόστος του χρόνου που απαιτείται για την εύρεση νέων διαδρομών. Το AODV αντιδρά γρήγορα στις αλλαγές τοπολογίας του δικτύου και ενημερώνει μόνο τους κόμβους που επηρεάζονται από τις αλλαγές αυτές. Τα "Hello Messages" που χρησιμοποιεί για τον έλεγχο των συνδέσεων είναι σχετικά περιορισμένα με αποτέλεσμα να μην αυξάνουν σημαντικά την κίνηση στο δίκτυο. Ένα ακόμα σημαντικό χαρακτηριστικό του AODV είναι και ο περιορισμός κατανάλωσης ενέργειας που επιτυγχάνει, αφού ο κόμβος

προορισμού απαντά μια φορά μόνο, στην πρώτη αίτηση και αγνοεί τις υπόλοιπες. Ο πίνακας δρομολόγησης διατηρεί το πολύ μία διαδρομή ανά προορισμό. Αν μία εγγραφή στον πίνακα δεν χρησιμοποιηθεί για συγκεκριμένο χρονικό διάστημα τότε παύει να ισχύει και διαγράφεται, όπως και μια μη έγκυρη διαδρομή.

Στα On - Demand πρωτόκολλα, εφαρμόζεται η τακτική κατά την οποία οι κόμβοι παρακολουθούν τη λειτουργία της δρομολόγησης και ενημερώνουν τον αποστολέα για πιθανά λάθη στην διαδρομή. Στην περίπτωση που υπάρχει διακοπή σε κάποια από τις συνδέσεις, ο κόμβος που θα το αντιληφθεί, στέλνει ένα "route error" πακέτο στον αποστολέα, ο οποίος με το που θα το παραλάβει, αφαιρεί από την cash όλες τις διαδρομές που περιέχουν την προβληματική σύνδεση και αμέσως ενεργοποιεί μια «διαδικασία εύρεσης διαδρομής». Ο αλγόριθμος AODV ελαχιστοποιεί τον αριθμό των μεταδόσεων με το να δημιουργεί της διαδρομές on - demand, όταν δηλαδή αυτές χρειάζονται, σε αντίθεση με άλλους αλγόριθμους που κάνουν το ακριβός αντίθετο.

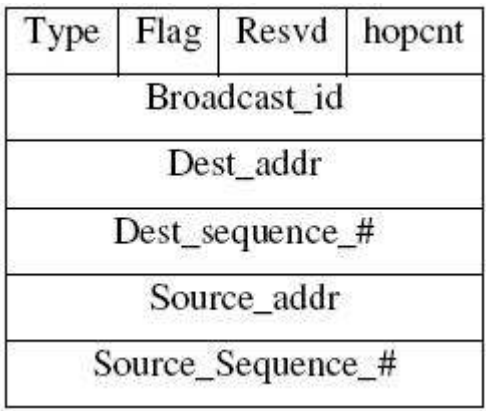
Μπορούμε να χωρίσουμε το πρωτόκολλο AODV σε δύο φάσεις:

- Στη φάση της ανακάλυψης διαδρομών και
- Στη φάση της συντήρησης ή διαχείρισης αυτών.

Οι κόμβοι δεν εκτελούν τις διαδικασίες εύρεσης διαδρομής ή «συντήρησης» αυτών, εκτός και πρέπει να επικοινωνήσουν με κάποιον άλλο κόμβο ή χρησιμοποιούνται ως ενδιάμεσοι κατά τη διάρκεια μιας διαδρομής πακέτου.

Τοπικά μηνύματα (Hello messages) χρησιμοποιούνται για τον έλεγχο της επικοινωνίας μεταξύ γειτονικών κόμβων, γεγονός που ελαττώνει το χρόνο απόκρισης σε αιτήσεις δρομολόγησης, αλλά και ενεργοποιεί τη διαδικασία ενημέρωσης όταν αυτό κρίνεται απαραίτητο.

Οι κόμβοι καθώς και οι εγγραφές στους πίνακες δρομολόγησης εμπεριέχουν ένα αύξοντα αριθμό ο οποίος χρησιμοποιείτε για τον εντοπισμό λανθασμένων εγγραφών. Κάθε κόμβος διαχειρίζεται δύο μετρητές, τον αύξοντα αριθμό του κόμβου (node sequence number) και το μετρητή μετάδοσης (broadcast ID). Όταν ένας κόμβος θελήσει να επικοινωνήσει με κάποιον άλλο για τον οποίο δεν έχει καταχωρημένη κάποια διαδρομή, μεταδίδει ένα πακέτο - αίτηση εύρεσης διαδρομής (route request packet) στους γειτονικούς κόμβους. Το πακέτο αυτό έχει την παρακάτω μορφή:



Εικόνα 13. *Πακέτο εύρεσης διαδρομής (AODV)*

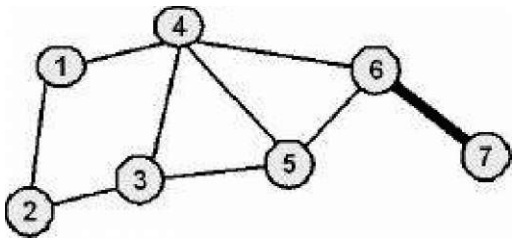
Όπου το Source _Sequence_# δηλώνει το πόσο πρόσφατη είναι η αντίστροφη διαδρομή προς την πηγή, ενώ το Dest_sequence_# δηλώνει αντίστοιχα το πόσο πρόσφατη είναι η διαδρομή για τον προορισμό. Τα Source_addr και Dest_addr, ορίζουν τη μοναδικότητα του αιτήματος εύρεσης διαδρομής.

Κάθε γειτονικός κόμβος που θα παραλάβει το πακέτο:

- Επιστρέφει ένα απαντητικό πακέτο δρομολόγησης (route reply packet) αν η πληροφορία για τη διαδρομή προς τον προορισμό υπάρχει στην cache του, ή
- Προωθεί το πακέτο του αιτήματος στους δικούς του γειτονικούς κόμβους.

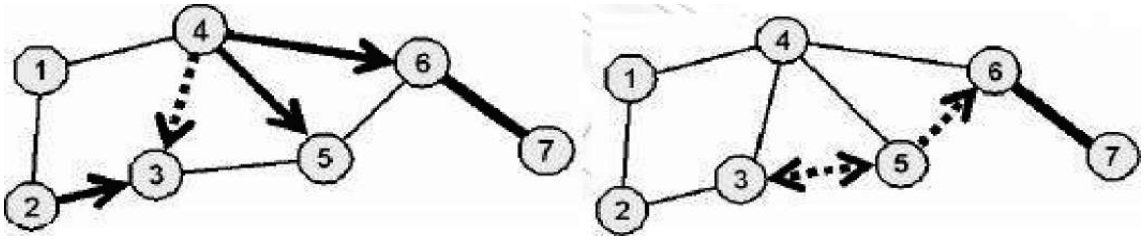
Όταν ένας κόμβος δεν μπορεί να απαντήσει στην αίτηση εύρεσης διαδρομής, τότε αυξάνει το μετρητή που αναφέρετε στον αριθμό των ενδιάμεσων κόμβων (hops) και αποθηκεύει τις πληροφορίες που έχουν να κάνουν με τη διαδρομή που θα ακολουθήσει το απαντητικό πακέτο (reverse path). Οι πληροφορίες που αποθηκεύονται είναι: Ο γειτονικός κόμβος που στέλνει το πακέτο - αίτησης εύρεσης διαδρομής, η IP διεύθυνση του κόμβου προορισμού, η IP διεύθυνση του κόμβου πηγής, ο αύξον αριθμός εκπομπής (broadcast ID), ο αριθμός του κόμβου πηγής(source node's sequence number) και ο χρόνος πέραν του οποίου παύει να ισχύει το αντίστροφο μονοπάτι (reverse path) για την αποφυγή συγκέντρωσης άχρηστων πληροφοριών.

Για παράδειγμα, ας υποθέσουμε ότι στο παρακάτω σχήμα, ο κόμβος 1 θέλει να στείλει δεδομένα στον κόμβο 7 και ο κόμβος 6 είναι ο μόνος που γνωρίζει πληροφορίες δρομολόγησης για τον συγκεκριμένο κόμβο.



Εικόνα 14.

Ο κόμβος 1 λοιπόν, στέλνει ένα αίτημα εύρεσης διαδρομής στους γειτονικούς κόμβους. Με τα εξής χαρακτηριστικά: Source_addr = 1, dest_addr = 7, broadcast_id = broadcast_id + 1, source_sequence_# = source_sequence_# + 1, dest_sequence_# = last dest_sequence_# για τον κόμβο 7. Οι κόμβοι 2 και 4 με τη σειρά τους αφού βεβαιωθούν ότι πρόκειται για νέα αίτηση εύρεσης διαδρομής, προωθούν το αίτημα αφού πρώτα ενημερώσουν το source_sequence_# για τον κόμβο 1 και αυξήσουν την τιμή στο hop_cnt του πακέτου. Έτσι το πακέτο φτάνει στον κόμβο 6 (από τον κόμβο 4), ο οποίος έχει πληροφορίες δρομολόγησης για τον κόμβο 7. Ο κόμβος 6 θα πρέπει να επιβεβαιώσει ότι το dest_sequence_# είναι μικρότερο ή ίσο από αυτό που ο ίδιος γνωρίζει για τον κόμβο 7. Οι κόμβοι 3 και 5 θα προωθήσουν το αίτημα στον κόμβο 6 ο οποίος και θα αναγνωρίσει ότι πρόκειται για το ίδιο αίτημα που έλαβε από τον κόμβο 4 (duplicate packets).



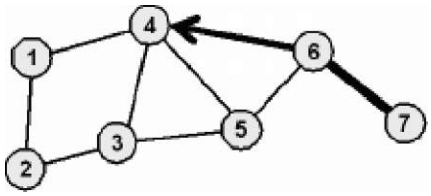
Εικόνα 15.

Έτσι αν κάποιος κόμβος παραλάβει ένα πακέτο - αίτηση εύρεσης νέας διαδρομής, η οποία περιέχει τη διαδρομή που μόλις ανακαλύφθηκε, τότε στέλνει ένα απαντητικό μήνυμα (route reply packet) στον γειτονικό κόμβο από τον οποίο παρέλαβε το αίτημα. Το απαντητικό μήνυμα έχει την παρακάτω μορφή:

Type	Flag	prsz	hopcnt
Dest_addr			
Dest_sequence_#			
Source_addr			
lifetime			

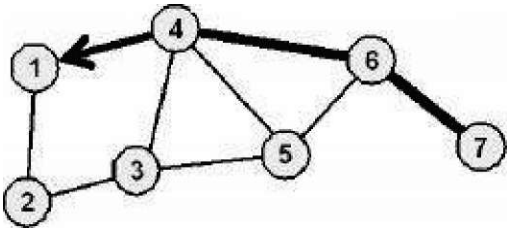
Εικόνα 16. *Η μορφή του Route Reply Packet στον AODV*

Οι ενδιάμεσοι κόμβοι μεταδίδουν την απάντηση έως την πηγή, χρησιμοποιώντας τις ανάστροφες διαδρομές δρομολόγησης που έχουν κρατήσει στην cache (cached reverse route entries). Άλλες αιτήσεις εύρεσης διαδρομής αγνοούνται, εκτός και το dest_sequence_# είναι μεγαλύτερο από το προηγούμενο ή το dest_sequence_# είναι το ίδιο αλλά το hop_cnt μικρότερο (σε αυτή την περίπτωση σημαίνει ότι υπάρχει συντομότερη διαδρομή). Τελικά η απάντηση στο ερώτημα εύρεσης διαδρομής φτάνει στον κόμβο ο οποίος και τη ζήτησε, που με τη σειρά του χρησιμοποιεί τους γείτονες που του απάντησαν ως επόμενους κόμβους για να στείλει το μήνυμά του στον κόμβο προορισμού. Έτσι για παράδειγμα ο κόμβος 6 που γνωρίζει μια διαδρομή για τον κόμβο 7 στέλνει απάντηση στον κόμβο 4 (route reply).



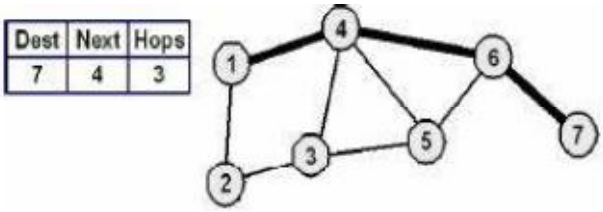
Εικόνα 17. *AODV Route Reply*

Στην περίπτωση αυτή θα έχουμε: Source_addr = 1, dest_addr = 7, dest_sequence_# = maximum (own sequence number, dest_sequence_# στο rout request), hop_cnt = 1. Ο κόμβος 4 πιστοποιεί ότι αυτή είναι μια νέα απάντηση στο ερώτημα εύρεσης διαδρομής (στη δική μας περίπτωση) ή μια απάντηση που έχει μικρότερο hop count και μεταδίδει το πακέτο στον κόμβο 1.



Εικόνα 18.

Επίσης αυξάνει το hop_cnt του πακέτου. Ο κόμβος 1 έχει πλέον μια έγκυρη διαδρομή για τον κόμβο 7 με 3 ενδιάμεσους κόμβους και μπορεί να τη χρησιμοποιήσει για να στείλει data.



Εικόνα 19.

Όπως είναι φυσικό η πιθανότητα να υπάρξουν αλλαγές δρομολόγησης είναι πάντα υπαρκτή και κάτι τέτοιο εντοπίζετε στην περίπτωση που υπάρχει αποτυχία κάποιου από τα περιοδικά "Hello Packets" που στέλνονται από κόμβο σε κόμβο ή αποτυχία στη μετάδοση πακέτου στον επόμενο κόμβο. Σε αυτήν την περίπτωση στέλνεται πίσω στον κόμβο πηγής ένα πακέτο λάθους δρομολόγησης (route error packet). Ο κόμβος πηγής ή οποιοσδήποτε άλλος κόμβος της διαδρομής μπορεί να δημιουργήσει ένα νέο μονοπάτι και να διορθώσει το λάθος στέλνοντας ένα νέο πακέτο - αίτημα εύρεσης διαδρομής.

Το πρωτόκολλο AODV είναι κατάλληλο για δυναμικά δίκτυα αλλά η αλήθεια είναι ότι υπάρχει καθυστέρηση στην δημιουργία των διαδρομών δρομολόγησης αφού π.χ. μια αποτυχία μετάδοσης, μπορεί να οδηγήσει σε μια προσπάθεια δημιουργίας νέας διαδρομής.

4.2 Μειονεκτήματα του Πρωτοκόλλου AODV

Είναι πιθανό για μια ενεργή διαδρομή να λήξη η περίοδος χρήσης της. Ο προσδιορισμός ενός λογικού χρονικού περιθωρίου, μετά το οποίο μια διαδρομή δεν θα πρέπει να χρησιμοποιείτε, είναι δύσκολη μιας και οι κόμβοι είναι κινητοί και το ποιος στέλνει που, δεν είναι δυνατόν να προβλεφθεί.

Το πρωτόκολλο AODV συγκεντρώνει ένα μικρό μόνο ποσοστό πληροφοριών δρομολόγησης. Αυτό με τη σειρά του προκαλεί πολλές φορές ένα κύμα από αιτήσεις εύρεσης διαδρομών που αρκετές φορές προκαλεί πρόβλημα στο δίκτυο (network overhead). Ένα τέτοιο κύμα που ξεφεύγει από τον έλεγχο δημιουργεί πολλές περιττές μεταδώσεις, με αποτέλεσμα το πρόβλημα να επιτείνεται.

Ένα άλλο σοβαρό μειονέκτημα του συγκεκριμένου πρωτοκόλλου (είναι κάτι που συναντούμε και σε πολλά άλλα πρωτόκολλα Ad - Hoc δικτύων) είναι και το γεγονός ότι

η απόδοσή του δεν είναι και τόσο ικανοποιητική όσο μεγαλύτερο γίνεται το δίκτυο. Η βασική διαφορά ενός μεγάλου από ένα μικρό δίκτυο είναι το μήκος του

μέσου μονοπατιού (average path length). Είναι λογικό ότι ένα μεγάλο μονοπάτι είναι περισσότερο ευάλωτο στο πρόβλημα των «κομμένων συνδέσεων» (link breakages). Επίσης όσο το μέγεθος ενός δικτύου μεγαλώνει, η απόδοση του πέφτει, μιας και αυξάνονται οι διεργασίες διαχείρισης (administrative load).

Το πρωτόκολλο AODV είναι ευάλωτο σε πολλών ειδών επιθέσεις ασφαλείας, μιας και βασίζεται στην εικασία ότι όλοι οι κόμβοι είναι σε θέση να συνεργαστούν μεταξύ τους. Χωρίς τη συνεργασία αυτή καμιά δρομολόγηση δεν μπορεί να υλοποιηθεί και κανένα πακέτο να αποσταλεί. Υπάρχουν δύο ειδών κόμβοι που αρνούντε τη συνεργασία με τους υπόλοιπους: οι κακόβουλοι (malicious) και αυτοί που επιδεικνύουν ιδιοτελή συμπεριφορά (selfish). Οι κακόβουλοι, είτε δεν μπορούν να ακολουθήσουν το πρωτόκολλο επικοινωνίας, είτε προσπαθούν με διάφορους τρόπους να επιτεθούν στο δίκτυο και τις λειτουργίες του. Οι κόμβοι με την ιδιοτελή συμπεριφορά δεν συμμετέχουν σε ορισμένες λειτουργίες του δικτύου (π.χ. απορρίπτουν πακέτα για να εξοικονομήσουν ενέργεια τα οποία θα μπορούσαν να αυξήσουν την αποτελεσματικότητα του δικτύου).

4.3 Ασφαλής Δρομολόγηση μέσο του AODV Πρωτοκόλλου

Για να προφυλάξει το δίκτυο από διάφορες κακόβουλες επιθέσεις, το πρωτόκολλο θα πρέπει να εκπληρώνει ένα σύνολο από προϋποθέσεις και να μπορεί να βεβαιώσει ότι το μονοπάτι που οδηγεί από την πηγή στον προορισμό θα λειτουργεί χωρίς πρόβλημα, ακόμα και στην περίπτωση παρουσίας κακόβουλων κόμβων. Ορισμένες από αυτές τις προϋποθέσεις είναι και οι εξής:

- Εξουσιοδοτημένοι κόμβοι θα πρέπει να εκτελούν τη διεργασία εύρεσης διαδρομής.

- Η αποκάλυψη της τοπολογίας του δικτύου θα πρέπει να είναι από μηδενική έως ελάχιστη.

- Το πρωτόκολλο θα πρέπει να είναι σε θέση να εντοπίζει σκοπίμως αλλοιωμένα μηνύματα δρομολόγησης.

- Θα πρέπει να υπάρχει μηχανισμός αποφυγής του φαινόμενου των άσκοπων κύκλων κατά τη δρομολόγηση των πακέτων (routing loops).

Ορισμένα από τα τρωτά σημεία του πρωτοκόλλου AODV είναι τα εξής:

- Η λανθασμένη αύξηση των μετρητών (sequence numbers): Οι μετρητές προορισμού (destination sequence numbers) φανερώνουν το πόσο «φρέσκια» είναι μια διαδρομή. Οι μετρητές αυτοί μεταβάλλονται, μόνο όταν ένα νεότερο πακέτο ελέγχου παραληφθεί, ο μετρητής του οποίου είναι μεγαλύτερος. Αυτό μπορεί να έχει ως αποτέλεσμα, ένας κακόβουλος κόμβος να αυξάνει το μετρητή αυτό, με σκοπό να επιβάλλει μια νέα διαδρομή για κάποιον προορισμό.

- Η δόλια μείωση του μετρητή ενδιάμεσων σταθμών (Hop Count): Το πρωτόκολλο AODV έχει ως ισχυρότερο κριτήριο για την επιλογή, το πόσο «φρέσκια» είναι μια διαδρομή, σε αντίθεση με το μήκος αυτής. Με άλλα λόγια ένας κόμβος θα προτιμούσε ένα πακέτο ελέγχου με μεγάλο αύξοντα αριθμό προορισμού και μετρητή ενδιάμεσων σταθμών, από ένα πακέτο με μικρότερο αύξοντα αριθμό προορισμού και μετρητή ενδιάμεσων σταθμών. Στην περίπτωση όμως που οι αύξοντες αριθμοί προορισμού είναι ίδιοι για δύο πακέτα ελέγχου, τότε η διαδρομή με το μικρότερο μετρητή ενδιάμεσων σταθμών επιλέγετε. Έτσι, ένας κακόβουλος κόμβος, θα μπορούσε να εκμεταλλευθεί το χαρακτηριστικό αυτό, μειώνοντας το μετρητή ενδιάμεσων σταθμών.

Η προσπάθεια να γίνει το πρωτόκολλο AODV περισσότερο ασφαλές χωρίστηκε σε τρεις κατηγορίες:

- Ανταλλαγή κλειδιού
- Ασφαλής Δρομολόγηση
- Προστασία Δεδομένων

Στις περισσότερες περιπτώσεις που έχουμε ανταλλαγή κλειδιού, έχουμε μια έμπιστη αρχή για την αρχική αυθεντικοποίηση. Μια παραλλαγή της κεντρικής αρχής είναι και το μοντέλο του Δημόσιου κλειδιού (Distributed Public - Key Model). Γενικά, η χρήση μιας κεντρικής έμπιστης οντότητας σε ένα τέτοιο δυναμικό περιβάλλον, μπορεί να θεωρηθεί από μη πρακτική έως και μη ασφαλής. Και αυτό γιατί μια οντότητα δεν μπορεί σε ένα τέτοιο περιβάλλον να είναι διαρκώς διαθέσιμη (π.χ. λόγω διακοπής στην επικοινωνία με κάποιο γειτονικό κόμβο). Ορισμένοι ερευνητές προτείνουν πριν την είσοδο του οποιουδήποτε κόμβου στο δίκτυο να πρέπει αυτός να παραλάβει ένα ζευγάρι δημόσιου και ιδιωτικού κλειδιού από την κεντρική οντότητα, όπως και να παραλάβει και το δημόσιο κλειδί της οντότητας αυτής. Μετά από αυτό, οι κόμβοι είναι σε θέση να ανταλλάσουν κλειδιά μεταξύ τους για την πραγματοποίηση της οποιασδήποτε επικοινωνίας, χωρίς την παρέμβαση της κεντρικής οντότητας, χρησιμοποιώντας οποιοδήποτε πρωτόκολλο ανταλλαγής κλειδιών κατάλληλο για Ad - Hoc δίκτυα. Αυτού του είδους τα κλειδιά είναι χρήσιμα για την ασφάλεια της διαδικασίας που έχει να κάνει με τη δρομολόγηση και φυσικά για την ασφαλή ροή των δεδομένων. Για να αποφευχθούν πολλαπλές peer to peer κρυπτογραφήσεις κατά τη διάρκεια μαζικών μεταδόσεων, χρησιμοποιείτε ένα «ομαδικό κλειδί» χρησιμοποιώντας το κατάλληλο πρωτόκολλο για την περίπτωση των ομαδικών κλειδιών. Στην περίπτωση αυτή έχει προταθεί η ιδέα να συμμετέχουν οι γειτονικοί κόμβοι σε μια διαμοιραζόμενη διαδικασία δημιουργίας ενός ζευγαριού RSA κλειδιού.

Το βασικό πρόβλημα ασφαλείας στα Ad - Hoc δίκτυα, είναι το γεγονός ότι οι ενδιάμεσοι κόμβοι συμμετέχουν στον καθορισμό των διαδρομών. Έτσι λοιπόν κρίνετε απαραίτητο μόνο εξουσιοδοτημένοι κόμβοι να έχουν τη δυνατότητα να μεταβάλλουν τα πακέτα που καθορίζουν τη διαδικασία δρομολόγησης, έτσι ώστε να αποφευχθεί η παρέμβαση από κακόβουλους κόμβους. Η συμμετρική peer to peer κρυπτογράφηση προτάθηκε από κάποιους ερευνητές, έτσι ώστε να απαγορεύσει την αλλαγή των πακέτων που έχουν να κάνουν με την δρομολόγηση από τους ενδιάμεσους κόμβους. Όλα λοιπόν τα πακέτα που έχουν να κάνουν με την δρομολόγηση, πρώτα κρυπτογραφούνται και μετά μεταδίδονται.

4.4 Βελτιώσεις Ασφαλείας για το Πρωτόκολλο AODV

Υπάρχουν δύο βασικοί τύποι επιθέσεων σε ένα Ad - Hoc δίκτυο που ακολουθεί το πρωτόκολλο AODV.

- Εσωτερικές Επιθέσεις
- Εξωτερικές Επιθέσεις

Οι εσωτερικές επιθέσεις πραγματοποιούνται από κακόβουλους ή ιδιοτελής (selfish) κόμβους. Κακόβουλοι είναι οι κόμβοι που μπορούν να αυθεντικοποιηθούν από τα δίκτυο ως νόμιμοι, με αποτέλεσμα να τους εμπιστεύονται οι υπόλοιποι, αλλά την ίδια στιγμή συμπεριφέροντε με τρόπο που δημιουργεί πρόβλημα. Ιδιοτελής είναι οι κόμβοι αυτοί που έχουν την τάση να αρνούνται την παροχή υπηρεσιών που έχουν να κάνουν με τη σωστή λειτουργία του δικτύου και των πρωτοκόλλων αυτού, με σκοπό να διατηρήσουν τους ίδιους πόρους.

Οι εξωτερικές επιθέσεις πραγματοποιούνται από κακόβουλους κόμβους. Οι κόμβοι αυτοί δεν μπορούν να αυθεντικοποιήσουν τους εαυτούς τους στο δίκτυο, λόγω του γεγονότος ότι δεν διαθέτουν τις σωστές κρυπτογραφικές πληροφορίες.

Διάφορα μοντέλα έχουν προταθεί τα οποία διαχειρίζονται τις επιθέσεις ασφαλείας. Ένα από τα γνωστότερα αποτελείτε από:

- Το μοντέλο εντοπισμού της επίθεσης
- Το μοντέλο άμυνας απέναντι στις επιθέσεις

Στο μοντέλο εντοπισμού επίθεσης κάθε κόμβος ενεργοποιεί ένα μοντέλο το οποίο παρακολουθώντας τις κινήσεις των διπλανών του, προσπαθεί να εντοπίσει πιθανή ύποπτη συμπεριφορά. Όταν το όριο της μη πρέπουσας συμπεριφοράς ξεπεραστεί για κάποιον από τους κόμβους, τότε η πληροφορία για το συγκεκριμένο κόμβο αποστέλλετε και στους υπόλοιπους. Το πρωτόκολλο εντοπισμού, εφαρμόζεται σε όλους τους κόμβους του δικτύου.

Στο μοντέλο άμυνας απέναντι στις επιθέσεις, όταν κάποιος κόμβος χαρακτηριστεί ως κακόβουλος, η πληροφορία αυτή μεταδίδετε σε ολόκληρο το δίκτυο μέσο ενός Mal πακέτου. Αν οποιοσδήποτε άλλος κόμβος υποπτεύεται τον ίδιο κόμβο ως κακόβουλο, τότε μεταδίδει στο δίκτυο ένα ReMal πακέτο. Αν αυτό συμβεί δύο ή περισσότερες φορές για ένα συγκεκριμένο κόμβο, τότε ο κόμβος απομονώνεται από το δίκτυο ως κακόβουλος, με τη μετάδοση ενός Purge πακέτου.

ΚΕΦΑΛΑΙΟ 5^{Ο}

5.1 Ασφάλεια Δικτύων Ad-Hoc

1)Εισαγωγή: Στα παρακάτω κεφάλαια αναπτύσσονται όλα τα θέματα ασφαλείας των δικτύων. Αυτά είναι τα χαρακτηριστικά της ασφαλείας που πρέπει να εφαρμοστούν για

να θεωρείται επιτυχής, τα είδη απειλών και επιθέσεων στα ad-hoc δίκτυα, καθώς και οι τρόποι αντιμετώπισης των απειλών.

5.2 Χαρακτηριστικά Ασφάλειας

Ο στόχος της ασφάλειας είναι να παρασχεθούν οι υπηρεσίες ασφάλειας που υπερασπίζουν το ad-hoc δίκτυο ενάντια σε όλα τα είδη απειλής που εξηγούνται σε αυτό το κεφάλαιο. Τα χαρακτηριστικά της ασφάλειας περιλαμβάνουν τα εξής:

- Διαθεσιμότητα

Η διαθεσιμότητα εξασφαλίζει την βιωσιμότητα των υπηρεσιών του δικτύου, παρά τις επιθέσεις denial of services (DoS) που δέχεται. Επίσης, τα συστήματα που εξασφαλίζουν τη διαθεσιμότητα προσπαθούν να καταπολεμήσουν τις επιθέσεις κατανάλωσης ενέργειας, καθώς επίσης την παρεκτροπή των κόμβων και την εγωιστική συμπεριφορά τους κατά την προώθηση μηνυμάτων. Οι παραπάνω απειλές θα παρουσιαστούν στη συνέχεια. Στο φυσικό επίπεδο, ένας αντίπαλος μπορεί να προκαλέσει συνωστισμό (jamming) για να παρέμβει στις επικοινωνίες. Στο επίπεδο δικτύου, μπορεί να διαταραχτεί το πρωτόκολλο προώθησης και να διακοπεί το δίκτυο. Σε ανώτερα επίπεδα μπορούν να ανατραπούν οι αντίστοιχες υπηρεσίες, όπως είναι η υπηρεσία διαχείρισης κλειδιού.

- Εμπιστευτικότητα

Η εμπιστευτικότητα εξασφαλίζει ότι η πληροφορία δεν εκτίθεται σε μη εξουσιοδοτημένες πηγές. Η μετάδοση ευαίσθητων πληροφοριών, όπως είναι στρατηγικές ή τακτικές στρατιωτικές πληροφορίες, απαιτεί εμπιστευτικότητα. Η διαρροή τέτοιων πληροφοριών σε εχθρούς σε περίοδο πολέμου αλλά και ειρήνης, όπως είναι οι στρατιωτικές ασκήσεις, μπορούν να έχουν καταστροφικές συνέπειες. Η πληροφορία δρομολόγησης πρέπει επίσης να μείνει εμπιστευτική σε ορισμένες περιπτώσεις γιατί αυτή μπορεί να είναι πολύτιμη για τον εχθρό ώστε να εξακριβώσει και να προσδιορίσει τους στόχους του στο πεδίο της μάχης. Η συνήθης τακτική για να κρατηθούν ευαίσθητα δεδομένα ασφαλή είναι η κρυπτογράφηση των δεδομένων με ένα μυστικό κλειδί, το οποίο μόνο οι επίδοξοι λήπτες κατέχουν. Επειδή η κρυπτογράφηση δημόσιου κλειδιού είναι πολύ ενεργοβόρα σε τέτοιου είδους δίκτυα, τα περισσότερα από τα προτεινόμενα πρωτόκολλα χρησιμοποιούν μεθόδους κρυπτογράφησης συμμετρικού κλειδιού.

- Αυθεντικότητα

Η αυθεντικότητα επιτρέπει σ' ένα κόμβο να διασφαλίσει την ταυτότητα του κάθε κόμβου κατά την διάρκεια της επικοινωνίας τους. Χωρίς την αυθεντικότητα, ένας αντίπαλος μπορεί να μεταμφιέσει έναν κόμβο και έτσι να κερδίσει μη εξουσιοδοτημένη πρόσβαση σε πηγές του δικτύου, σε ευαίσθητες πληροφορίες και να παρέμβει στις λειτουργίες άλλων κόμβων. Έτσι, η αυθεντικότητα είναι απαραίτητη για πολλούς εκτελεστικούς σκοπούς του προγράμματος, όπως εκ νέου προγραμματισμός του δικτύου, έλεγχος κύκλου ασφαλείας σ' ένα κόμβο κ.ά. Η αυθεντικότητα πληροφορίας επιτρέπει στον δέκτη να επιβεβαιώσει ότι η πληροφορία στάλθηκε τοπικά από τον πραγματικό αποστολέα. Η αυθεντικότητα μπορεί να επιτευχθεί με έναν καθαρά συμμετρικό μηχανισμό. Ο αποστολέας και ο λήπτης μοιράζονται ένα μυστικό κλειδί με το οποίο υπολογίζουν έναν κώδικα αυθεντικότητας μηνύματος (message authentication code -

MAC) για όλα τα αποστελλόμενα δεδομένα. Όταν ένα μήνυμα με τον σωστό MAC φτάσει, ο λήπτης ξέρει την ταυτότητα του αποστολέα. Όμως, κατά την εκπομπή μηνύματος προς πολλούς αποδέκτες, χρειάζονται ισχυρότεροι δεσμοί εμπιστοσύνης. Σε αυτή την περίπτωση, μπορούν να χρησιμοποιηθούν άλλες τεχνικές όπως είναι τα πρωτόκολλα SPINS και LEAP.

- Μη αποποίηση

Η απαίτηση της μη αποποίησης εξασφαλίζει ότι ο αποστολέας ενός μηνύματος δεν μπορεί να αρνηθεί ότι έχει στείλει το μήνυμα. Η μη αποποίηση είναι χρήσιμη στην επισήμανση και απομόνωση εκτεθειμένων κόμβων. Έτσι, όταν ένας κόμβος Α δέχεται ένα λανθασμένο μήνυμα από έναν κόμβο Β, η μη αποποίηση επιτρέπει στον Α να κατηγορήσει τον Β ότι αυτός έστειλε το μήνυμα και να πείσει τους υπόλοιπους κόμβους του δικτύου ότι ο Β είναι εκτεθειμένος. Οι ψηφιακές υπογραφές μπορεί να είναι μία λύση για την παραπάνω περίπτωση.

- Ανανέωση Δεδομένων

Η απαίτηση για ανανέωση των δεδομένων δηλώνει ότι οι πληροφορίες και τα μηνύματα που ανταλλάσσονται είναι έγκυρα και διαβεβαιώνει ότι δεν επαναλαμβάνεται αναμετάδοση παλαιών μηνυμάτων. Σε όλα τα μηνύματα, συνήθως, παρέχεται ένας καταμετρητής χρόνου. Βάσει του μετρητή μπορούμε να διασφαλίσουμε ότι η πληροφορία που λαμβάνουμε είναι καινούρια. Ένας κοινός τρόπος αντιμετώπισης απειλών είναι να περιλάβουμε έναν αυξανόμενο μετρητή με κάθε μήνυμα το οποίο στέλνεται και να απορρίψουμε μηνύματα με παλαιές τιμές του μετρητή. Επίσης η ανανέωση μπορεί να αφορά στην ανανέωση του κλειδιού που χρησιμοποιείται για την κρυπτογράφηση των δεδομένων. Στην περίπτωση αυτή, κάθε κλειδί βεβαιωμένης μεθόδου μπορεί να βεβαιώσει ότι το διαμοιραζόμενο κλειδί ανάμεσα στους εμπλεκόμενους είναι καινούργιο.

- Ακεραιότητα πληροφορίας

Η ακεραιότητα πληροφορίας δηλώνει την γνησιότητα των δεδομένων που στέλνονται μεταξύ εμπλεκομένων. Έτσι, ένα μήνυμα που στέλνεται από έναν κόμβο Α σ' ένα κόμβο Β δεν έχει τροποποιηθεί από έναν κακόβουλο κόμβο Γ κατά τη διάρκεια της μετάδοσης. Ένα μήνυμα μπορεί επίσης να τροποποιηθεί ή να καταστραφεί λόγω εξασθένησης του σήματος. Η υπηρεσία της ακεραιότητας πληροφορίας παρέχεται συχνά από την υπηρεσία της αυθεντικότητας ώστε να εξασφαλιστεί η ασφάλεια του δικτύου. Ένα καλό και ασφαλές σύστημα θα ήταν ικανό να ανιχνεύσει οποιοδήποτε πρόβλημα ακεραιότητας ώστε αν μια παράβαση διαπιστωθεί, τότε άμεσα η υπηρεσία να αναφέρει αυτό το πρόβλημα.

- Επεκτασιμότητα

Συνήθως τα δίκτυα που εξετάζουμε χρειάζονται επέκταση με προσθήκη μεγάλου αριθμού νέων κόμβων. Η ανάγκη αυτή απαιτεί δίκτυα τα οποία να μπορούν να έχουν ιδιότητες επέκτασης, είτε ως προς το ενεργειακό μέρος είτε ως προς το θέμα αναδιοργάνωσης του δικτύου. Ο αριθμός των γειτόνων, οι αποστάσεις μεταξύ τους και η απαιτούμενη ισχύς για την αποστολή μηνυμάτων από έναν κόμβο στον άλλο, πιθανόν να μην είναι γνωστά κατά τη διάρκεια ζωής ενός δικτύου. Έτσι οι κόμβοι στα υπό εξέταση

δίκτυα πρέπει να είναι ικανοί να αυτό-οργανώνονται και να επιλέγουν τους κατάλληλους μηχανισμούς που ταιριάζουν σε κάθε περίσταση.

- Συνεργασία

Εκτός από την ασφαλή αποστολή και λήψη μηνυμάτων, η υποκίνηση της συνεργασίας είναι ένα σημαντικό θέμα ασφαλείας. Λόγω του περιορισμένου αριθμού πηγών του δικτύου, οι συσκευές του δικτύου τείνουν να γίνουν εγωκεντρικές. Έτσι χρειάζεται ένα είδος υποκίνησης για να παρακινηθεί η συνεργασία στο δίκτυο. Πολλές μέθοδοι δουλεύουν δίνοντας κίνητρο για επιτυχή συνεργασία, ενώ άλλες τιμωρούν την εγωιστική συμπεριφορά.

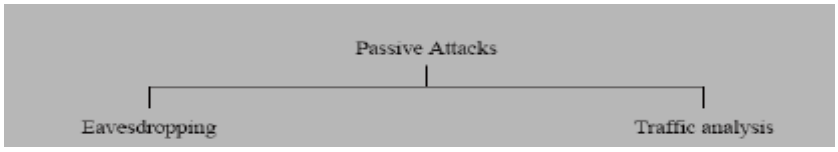
5.3 Επιθέσεις κατά δικτύων Ad-Hoc

Οι επιθέσεις ασφάλειας μπορούν να ταξινομηθούν σε δύο ευρείες κατηγορίες: ενεργητικές και παθητικές επιθέσεις. Στις παθητικές επιθέσεις, οι αντίπαλοι δεν κάνουν καμιά εκπομπή, είναι κυρίως ενάντια στην εμπιστευτικότητα των στοιχείων του μηνύματος. Στις ενεργές επιθέσεις, οι κακόβουλες πράξεις πραγματοποιούνται όχι μόνο ενάντια στην εμπιστευτικότητα αλλά και στην ακεραιότητα των στοιχείων.

Οι ενεργές επιθέσεις μπορούν επίσης να στοχεύσουν τη μη εξουσιοδοτημένη πρόσβαση και τη χρήση των πόρων ή τη διαταραχή των επικοινωνιών ενός αντιπάλου.

Από ένα λάθος, οι χρήστες μπορούν να εκθέσουν τους κόμβους στις απειλές όπως να πειράξουν και να καταστρέψουν ή να εκθέσουν στοιχεία σε όσους δεν έχουν εξουσιοδοτημένη πρόσβαση. Τα συστήματα ασφάλειας πρέπει επίσης να αντιμετωπίσουν τις προκλήσεις προστασίας και ασφάλειας που δημιουργούνται από την απρόσεκτη χρήση κατά την διάρκεια κάποιων γεγονότων

1)Παθητικές Επιθέσεις: Στις παθητικές επιθέσεις οι επιτιθέμενοι είναι χαρακτηριστικά καλυμμένοι και εισέρχονται στις γραμμές επικοινωνίας για να συλλέξουν τα στοιχεία της πληροφορίας που θέλουν. Οι παθητικές επιθέσεις (σχήμα 4) μπορούν να ομαδοποιηθούν σε δύο διαφορετικούς τύπους. Σε αυτούς που «κρυφακούν» και σε αυτούς που αναλύουν την κυκλοφορία.



Εικόνα 20. *Παθητικές Επιθέσεις*

Eavesdropping

Τα ταξινομημένα στοιχεία μπορούν να κρυφακουστούν με την υποκλοπή των γραμμών επικοινωνίας, για το λόγο αυτό οι ασύρματες συνδέσεις είναι ευκολότερες σε τέτοιου είδους επιθέσεις. Όταν είναι γνωστά τα πρότυπα τα οποία χρησιμοποιούνται για τα

δεδομένα, δηλαδή μη κρυπτογραφημένα, ένας αντίπαλος μπορεί εύκολα να λάβει και να διαβάσει τα στοιχεία που μεταδίδονται μέσω των οπτικοακουστικών μεταδόσεων. Παραδείγματος χάριν, ένας αντίπαλος μπορεί εύκολα να κρυφακούσει τους αριθμούς και τους κωδικούς πρόσβασης πιστωτικών καρτών όταν διαβιβάζονται απλά πέρα από τις ανασφαλείς ασύρματες συνδέσεις.

Πραγματικά, τα ad hoc δίκτυα και τα δίκτυα αισθητήρων είναι πιο ασφαλή ενάντια στην υποκλοπή έναντι άλλης ασύρματης τεχνολογίας επειδή τα σήματα δεν στέλνονται πέρα από τις πιο σύντομες αποστάσεις. Ένας αντίπαλος πρέπει να φτάσει αρκετά κοντά στον επιτιθέμενο κόμβο για να είναι σε θέση να υποκλέψει κάποια δεδομένα. Εάν το μέσο όπου αυτές οι ασύρματες τεχνολογίες χρησιμοποιούν έχουν αρκετό διάστημα ελέγχου ενάντια στους εισβολείς, δηλαδή σε ανθρώπους και συσκευές που δεν έχουν εξουσιοδότηση, αυτά γίνονται ασφαλέστερα. Ένα μέλος το οποίο είναι κοντά στο τερματικό που είναι στόχος μπορεί να λάβει όλα τα πλαίσια τα οποία στέλνει ή λαμβάνει, να τα αποθηκεύσει σε κάποιο μέσο και να τα πάρει. Αυτοί οι κίνδυνοι μπορούν να μειωθούν από τις προσεκτικές επιθεωρήσεις ή με τον έλεγχο των ηλεκτρομαγνητικών εκπομπών από το μέσο. Ακόμα, οι κίνδυνοι είναι πολύ υψηλότεροι όταν χρησιμοποιούνται οι ασύρματες τεχνολογίες.

Επιπλέον, η ύπαρξη των ασύρματων επικοινωνιών καθιστά την εφαρμογή των πολλαπλών δικτύων με τα διαφορετικά επίπεδα ασφάλειας σε μια δυσκολότερη ενιαία εγκατάσταση. Παραδείγματος χάριν, εάν υπάρχουν ταξινομημένα δίκτυα και ένα δίκτυο που συνδέεται με το Διαδίκτυο στο ίδιο μέσο και η ασύρματη πρόσβαση στα ταξινομημένα δίκτυα επιτρέπεται, με την αποσύνδεση του Διαδικτύου τα ταξινομημένα δίκτυα μπορούν να γίνουν πολύ δύσκολα στις παθητικές επιθέσεις.

Για την προστασία της μυστικότητας, η ανωνυμία είναι σημαντική. Οι επιθέσεις ενάντια στη μυστικότητα μπορούν να αρχίσουν με τις επιθέσεις ενάντια στην ανωνυμία. Ένας αντίπαλος πρώτα πρέπει να ξέρει ποιος κόμβος εξυπηρετεί ποιο άτομο και για ποιο σκοπό. Ομοίως, πρέπει να ξέρει ποιο πακέτο στοιχείων προέρχεται από ποιο κόμβο. Αφότου επιτυγχάνεται αυτό, τα στοιχεία που συλλέγονται μπορούν να γίνουν σημαντικότερα. Επομένως, η μυστικότητα και η εμπιστευτικότητα μπορούν να ενισχυθούν από την ανωνυμία. [9]

Traffic analysis

Όπως και το περιεχόμενο των δεδομένων των πακέτων, η ανάλυση της κυκλοφορίας μπορεί επίσης να είναι πολύ σημαντική για τους αντιπάλους. Παραδείγματος χάριν, οι σημαντικές πληροφορίες για την τοπολογία δικτύωσης μπορούν να παραχθούν με την ανάλυση της κυκλοφορίας. Στα ad hoc δίκτυα και ειδικά στα δίκτυα αισθητήρων, οι κόμβοι που βρίσκονται πιο κοντά στο σταθμό βάσης, κάνουν περισσότερες μεταδόσεις από τους άλλους κόμβους επειδή αναμεταδίδουν περισσότερα πακέτα από τους κόμβους που βρίσκονται μακριά από το σταθμό βάσης. Ομοίως, η ομαδοποίηση (clustering) είναι ένα σημαντικό εργαλείο για την εξελιξιμότητα στα ad hoc δίκτυα και οι επικεφαλείς των ομάδων είναι πιο πολυάσχολοι από τους άλλους κόμβους στο δίκτυο. Οι κόμβοι που βρίσκονται κοντά σε ένα σταθμό βάσης ή οι επικεφαλείς των συστάδων μπορεί να είναι πολύ χρήσιμοι για τους αντιπάλους επειδή μια επίθεση DoS ενάντια σε αυτούς τους κόμβους μπορεί να ασκήσει μεγαλύτερη επίδραση στο δίκτυο. Με την ανάλυση της κυκλοφορίας, αυτό το είδος πολύτιμων πληροφοριών μπορεί να παραχθεί.
Η ανάλυση κυκλοφορίας μπορεί επίσης να χρησιμοποιηθεί για να οργανώσει τις επιθέσεις ενάντια στην ανωνυμία. Η ανίχνευση των κόμβων της πηγής για ορισμένα πακέτα δεδομένων μπορεί επίσης να είναι ένας στόχος για τους αντιπάλους. Αυτές οι

πληροφορίες βοηθούν να ανιχνεύσουν τη θέση των γεγονότων, τις αδυναμίες, τις ικανότητες και τις λειτουργίες του δικτύου ή τους ιδιοκτήτες των κόμβων.

Επιπλέον, τα δείγματα της κυκλοφορίας μπορούν να αναφέρονται και σε άλλες εμπιστευτικές πληροφορίες όπως οι ενέργειες και οι προθέσεις. Στις τακτικές επικοινωνίες, η σιωπή μπορεί να δείξει την προετοιμασία για μια επίθεση, μια τακτική κίνηση ή μια διήθηση. Ομοίως, μια ξαφνική αύξηση στο ποσοστό κυκλοφορίας μπορεί να δείξει την έναρξη μιας σκόπιμης επίθεσης ή μιας επιδρομής. Οι παρόμοιες πληροφορίες μπορούν επίσης να παραχθούν από την ανάλυση κυκλοφορίας στα δίκτυα. Η ανάλυση κυκλοφορίας μπορεί να πραγματοποιηθεί για να απαριθμήσει τις συχνές επαφές κάθε τερματικού - αποκαλούμενου friendship trees. Με τον τρόπο αυτό, οι επαφές ενός κόμβου μπορούν να καθοριστούν.

Μια από τις ακόλουθες τεχνικές μπορεί να χρησιμοποιηθεί για την ανάλυση κυκλοφορίας:

Α) **Ανάλυση κυκλοφορίας στο φυσικό στρώμα:** σε αυτήν την επίθεση μόνο ο μεταφορέας αισθάνεται την επίθεση και τα ποσοστά κυκλοφορίας αναλύονται για τους κόμβους σε μια θέση.

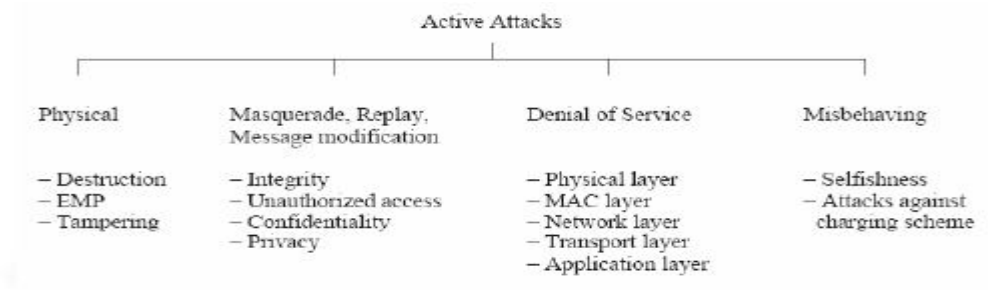
Β) **Ανάλυση κυκλοφορίας στη MAC και τα υψηλότερα στρώματα:** Τα πλαίσια της MAC και τα πακέτα δεδομένων μπορούν να υποπολλαπλασιαστούν και οι επιγραφές μπορούν να αναλυθούν. Αυτό μπορεί να αποκαλύψει διάφορες πληροφορίες δρομολόγησης καθώς και την τοπολογία του δικτύου.

Γ) **Ανάλυση κυκλοφορίας από το συσχετισμό γεγονότος:** γεγονότα όπως η ανίχνευση σε ένα δίκτυο αισθητήρων ή τη μετάδοση από ένα χρήστη μπορεί να συσχετιστεί με την κυκλοφορία και περισσότερες αναλυτικές πληροφορίες, μπορούν να παραχθούν.

Δ) **Ενεργός ανάλυση κυκλοφορίας:** η ανάλυση κυκλοφορίας μπορεί επίσης να διευθυνθεί ως ενεργός επίθεση. Παραδείγματος χάριν, ορισμένοι κόμβοι μπορούν να καταστραφούν, το οποίο υποκινεί το self organize στο δίκτυο, και τα πολύτιμα στοιχεία για την τοπολογία μπορούν να συγκεντρωθούν.[4]

Ενεργές Επιθέσεις

Στις ενεργές επιθέσεις ένας αντίπαλος έχει επιπτώσεις πραγματικά στις διαδικασίες στο επιτεθειμένο δίκτυο. Αυτή η επίδραση μπορεί να είναι ο στόχος της επίθεσης και μπορεί να ανιχνευθεί. Παραδείγματος χάριν, οι υπηρεσίες δικτύωσης μπορούν να υποβιβαστούν ή να τερματίσουν ως συνέπεια αυτών των επιθέσεων. Μερικές φορές ο αντίπαλος προσπαθεί να μείνει μη ανιχνεύσιμος, στοχεύοντας να κερδίσει την πρόσβαση στους πόρους των συστημάτων ή απειλώντας την εμπιστευτικότητα ή και την ακεραιότητα του περιεχομένου του δικτύου. Ομαδοποιούμε τις ενεργές επιθέσεις σε τέσσερις κατηγορίες, όπως φαίνεται στο παρακάτω σχήμα (σχήμα 21).[10]



Εικόνα 21.*Ενεργές Επιθέσεις*

Physical Attack

Ένας αντίπαλος μπορεί φυσικά να βλάψει το hardware προκειμένου να εξοντώσει τους κόμβους. Αυτό είναι μια επίθεση ασφάλειας η οποία μπορεί να θεωρηθεί μέσα στα επιτρεπτά όρια της ανοχής ελαττωμάτων, στην οποία υπάρχει η δυνατότητα να στηριχτούν οι λειτουργίες δικτύωσης χωρίς οποιαδήποτε διακοπή λόγω των αποτυχιών των κόμβων. Οι φυσικές επιθέσεις ενάντια στο hardware είναι ένα σοβαρό ζήτημα, ειδικά στις ad hoc επικοινωνίες και τα δίκτυα αισθητήρων. Οι κόμβοι αισθητήρων μπορούν να επεκταθούν αφύλακτοι σε περιοχές προσιτές από τον αντίπαλο. Επομένως, μπορούν να κινηθούν έξω από την περιοχή αισθητήρων ή να καταστραφούν. Όταν αυτοί οι κίνδυνοι είναι επικείμενοι, οι κόμβοι πρέπει να είναι ελαστικοί στις φυσικές επιθέσεις.

Όταν οι κόμβοι είναι αφύλακτοι και μπορεί ο αντίπαλος να έρθει σε επαφή, οι κόμβοι μπορούν να δεχθούν επίθεση με τεχνικές αλλοίωσης. Επομένως, η ανθεκτικότητα πλαστογραφήσεων είναι ένα ζήτημα που πρέπει να εξεταστεί προσεκτικά τόσο σε δίκτυα αισθητήρων και ad hoc όσο και σε εφαρμογές τακτικών επικοινωνιών.

Μπορούμε να ομαδοποιήσουμε τους κόμβους με βάση την τεχνική της αλλοίωσης σε δύο κατηγορίες: της επεμβατικής και της μη επεμβατικής αλλοίωσης. Οι επεμβατικές τεχνικές στοχεύουν να κερδίσουν την απεριόριστη πρόσβαση σε ένανκόμβο. Στις μη επεμβατικές επιθέσεις, η απεριόριστη πρόσβαση στον κόμβο δεν είναιη πρόθεση. Αντίθετα, αναλύοντας τη συμπεριφορά ενός κόμβου, όπως η κατανάλωσηενέργειας ή τις ρυθμίσεις χρονισμού εκτέλεσης των αλγορίθμων για διάφορεςεισροές, μπορούν να προκύψουν εμπιστευτικά δεδομένα σχετικά με τις διαδικασίες και τα κλειδιά που χρησιμοποιούνται από τα συστήματα κρυπτογράφησης.

Οι επιθέσεις ηλεκτρομαγνητικών παλμών (EMP) είναι επίσης μεταξύ των απειλών που μπορούν να παρατίθενται στις επιθέσεις φυσικής ασφάλειας. Μια EMP είναι μια μικρής διάρκειας καταιγισμού υψηλής έντασης ηλεκτρομαγνητική ενέργεια που μπορεί να οδηγήσει σε απότομες αυξομειώσεις της τάσης και να καταστρέψει ηλεκτρονικές συσκευές εντός μιας συγκεκριμένης εμβέλειας. Μια EMP είναι ένα φυσικό αποτέλεσμα πυρηνικών εκρήξεων. Σήμερα, φορητές συσκευές που μπορούν να δημιουργήσουν EMPs είναι διαθέσιμες. Αν και υπάρχουν ακόμη άλυτα ζητήματα που σχετίζονται με το εφικτό EMP τεχνολογιών, είναι μια απειλή για όλα τα είδη των ηλεκτρικών συσκευών σε πεδίο τακτικής. Αυτό μπορεί να θεωρηθεί ως μέρος του τομέα ανοχής σφαλμάτων. Είναι δυνατή η δημιουργία ηλεκτρονικών συσκευών που είναι πιο ανθεκτική σε EMPs. Ως εκ τούτου, θα τοποθετήσουμε τις EMP επιθέσεις ως τύπος επίθεσης ασφαλείας.

Masquerade, Replay and Message Modification

Ένας μεταμφιεσμένος κόμβος ενεργεί σαν είναι ένας άλλος κόμβος. Τα μηνύματα μπορούν να ληφθούν και να επαναληφθούν μέσω των κόμβων αυτών. Τέλος, το περιεχόμενο των ληφθέντων μηνυμάτων μπορεί να τροποποιηθεί πριν γίνει η επανάληψη τους. Διάφορα σενάρια και απειλές μπορούν να αναπτυχθούν με βάση αυτές τις προσεγγίσεις.

Τα δίκτυα Ad hoc και τα δίκτυα αισθητήρων εισάγουν τα ιδιαίτερα πλεονεκτήματα για την μεταμφίεση των κόμβων. Στα ad hoc δίκτυα, οι κόμβοι μπορούν να αλλάξουν τη θέση τους στο δίκτυο ανά τακτά χρονικά διαστήματα. Δεδομένου ότι οι αντιδραστικές τεχνικές προτιμώνται για τη δρομολόγηση, η τοπολογία δεν μπορεί να διατηρηθεί, κάνοντάς το δύσκολο να ελεγχθεί και αυτό έχει σαν συνέπεια να είναι δύσκολο το σημείου πρόσβασης ενός κόμβου στο δίκτυο. Επιπλέον, μπορεί να μην είναι δυνατό να ελεγχθεί εάν ο κόμβος έχει πρόσβαση ήδη σε ένα άλλο σημείο του δικτύου. Αντ' αυτού όμως, τεχνικές όπως το στοιχείο-κεντρικής δρομολόγησης και της επαναχρησιμοποίησης διευθύνσεων μπορούν να είναι σχέδιο εξέτασης.

Η μεταμφίεση, η επανάληψη μηνυμάτων και η τροποποίηση περιεχομένου μπορούν να χρησιμοποιηθούν για να επιτεθούν στην ακεραιότητα του περιεχομένου των μηνυμάτων ή των υπηρεσιών σε ένα δίκτυο. Τα δίκτυα αισθητήρων, συγκεκριμένα, έχουν διάφορες λειτουργίες δικτύων οι οποίες είναι ευαίσθητες στα πρόσθετα είδη επίθεσης επειδή είναι βασισμένες σε μια συνεργασμένη προσπάθεια των κόμβων. Παραδείγματος χάριν, τα σχέδια εντοπισμού κόμβων μπορούν να υπόκεινται σε μια από τις ακόλουθες επιθέσεις ασφάλειας:

- Ένας κακόβουλος κόμβος μπορεί να ενεργήσει ως αναγνωριστικό σήμα και να διαδώσει τη θέση του λανθασμένα. Αυτό παρακωλύει τη διαδικασία εντοπισμού του κόμβου όταν αυτός χρησιμοποιεί σήματα τα οποία εκπέμπονται από τον κακόβουλο κόμβο.
- Ένα αναγνωριστικό σήμα μπορεί να αλλαχθεί και να εισαγάγει λανθασμένα στοιχεία θέσης, να διαβιβάσει αναγνωριστικά σήματα με λιγότερη ή περισσότερη ενίσχυση από το αναμενόμενο για να εξασθενίσει την λαμβανόμενη ενίσχυση του σήματος του δέκτη.
- Τα αναγνωριστικά σήματα μπορούν να επαναληφθούν από έναν κακόβουλο κόμβο.
- Οι κόμβοι αναγνωριστικών σημάτων μπορούν να καταστραφούν από τις φυσικές επιθέσεις.
- Ένα εμπόδιο μπορεί να τοποθετηθεί μεταξύ των κόμβων αναγνωριστικών σημάτων και του δικτύου για να εμποδίσει την άμεση σύνδεση.

Μια βελτιωμένη έκδοση της μεταμφίεσης είναι μια επίθεση sybil, όπου ένας κακόβουλος κόμβος εισάγει τον εαυτό του πολλαπλά στο δίκτυο. Η κατοχή των πολλαπλών προσδιορισμών μπορεί να είναι πολύ χρήσιμη για έναν κακόβουλο κόμβο. Ένας κόμβος που στέλνει πολλαπλές τιμές με τους διαφορετικούς προσδιορισμούς μπορεί να αλλάξει την συνολική αξία σημαντικά. Μια επίθεση sybil μπορεί επίσης να απειλήσει τις πολλαπλές δρομολογήσεις καθώς και τον εντοπισμό των κόμβων, κ.λπ. Τέλος, μπορούν επίσης να βοηθήσουν να κρατήσουν τις επιθέσεις κρυμμένες.

Η μεταμφίεση, η επανάληψη των μηνυμάτων και η τροποποίηση περιεχομένου μπορούν επίσης να χρησιμοποιηθούν ενάντια στην εμπιστευτικότητα κάνοντας τους υπόλοιπους

κόμβους να στέλνουν εμπιστευτικά στοιχεία σε έναν κακόβουλο κόμβο και με τον τρόπο αυτό να του παρέχεται πρόσβαση σε όλους τους πόρους του συστήματος.

Ένας αντίπαλος κάνει phishing, το οποίο σημαίνει ότι εξαπατά κάποιον κόμβο προκειμένου να του δώσει τις εμπιστευτικές πληροφορίες εθελοντικά. Ο όρος αυτός είναι ένας συνδυασμός δύο λέξεων - κωδικός πρόσβασης και phishing - που καθορίζουν αυτήν την επίθεση. Ένας κακόβουλος κόμβος υποδύεται ότι είναι ένας εξουσιοδοτημένος κόμβος και μπορεί να ζητήσει από έναν άλλο κόμβο να του δώσει πληροφορίες για τους κωδικούς πρόσβασης, τα κλειδιά, κ.λπ.

Η μεταμφίεση είναι επίσης μια προσέγγιση για τη συντήρηση της ανωνυμίας ενός κακόβουλου κόμβου που παρέχει το παράνομο περιεχόμενο, ή ένας που επιτίθενται ή κερδίζει στην παράνομη πρόσβαση σε ένα μακρινό σύστημα, π.χ. μια σημαντική βάση δεδομένων της κυβέρνησης ή των τραπεζών.

Denial of Service Attacks

Μια επίθεση άρνησης υπηρεσιών (DoS) στοχεύει κυρίως στη διαθεσιμότητα των υπηρεσιών δικτύων. Ένα DoS ορίζεται ως οποιοδήποτε γεγονός που μικραίνει την ικανότητα ενός δικτύου να εκτελέσει την αναμενόμενη λειτουργία του σωστά ή κατά τρόπο έγκαιρο (Wood και Stankovic, 2005). Μια επίθεση DoS χαρακτηρίζεται από τις ακόλουθες ιδιότητες:

- Κακόβουλος: πραγματοποιείται για να αποτρέψει το δίκτυο από την πραγματοποίηση των προοριζόμενων λειτουργιών του. Δεν είναι τυχαίο και δεν ανήκει στην περιοχή ανοχής της ασφάλειας και των ελαττωμάτων.
- Αποδιοργανωτικός: υποβιβάζει την ποιότητα των υπηρεσιών που προσφέρονται από το δίκτυο.
- Ασύμμετρος: ο επιτιθέμενος υποβάλλει την λιγότερη προσπάθεια έναντι της κλίμακας του αντίκτυπου που έχει στο δίκτυο. Κάθε υπηρεσία δικτύωσης μπορεί να υπόκειται σε μια επίθεση DoS.

Σε αυτό το τμήμα θα εξετάσουμε τα σημαντικά σενάρια DoS για τα Ad Hoc δίκτυα.

A) DoS in Physical Layer

Σε αυτό το τμήμα, το φυσικό στρώμα δείχνει το στρώμα του μοντέλου του OSI που είναι αρμόδιο για να αντιπροσωπεύσει τα σωστά 1s και 0s στο ασύρματο μέσο, και μια επίθεση DoS στο φυσικό στρώμα, που καλείται παρεμβολή παρασίτων, σημαίνει μια απειλή ασφάλειας ενάντια σε αυτό.

Μια κακόβουλη συσκευή μπορεί να φράξει έναν ασύρματο μεταφορέα με τη διαβίβαση ενός σήματος σε εκείνη την συχνότητα. Τα παράσιτα συμβάλλουν στο θόρυβο του φέροντος και η δύναμή τους είναι αρκετή να μειώσει το σήμα κάτω από το επίπεδο που οι κόμβοι που χρησιμοποιούν εκείνη την στιγμή τα κανάλια να παραλαμβάνουν σωστά τα δεδομένα. Η παρεμβολή παρασίτων μπορεί να διευθυνθεί συνεχώς σε μια περιοχή, η οποία ανατρέπει όλους τους κόμβους σε εκείνη την περιοχή από την επικοινωνία. Εναλλακτικά, η παρεμβολή παρασίτων μπορεί να γίνει προσωρινά με τυχαία χρονικά διαστήματα, τα οποία μπορούν ακόμα πολύ αποτελεσματικά να παρακωλύσουν τις μεταδόσεις.

Β) DoS in the Link Layer

Οι αλγόριθμοι στο στρώμα συνδέσεων, ειδικά της MAC, παρουσιάζουν πολλές ευκαιρίες εκμετάλλευσης για τις επιθέσεις DoS. Παρακάτω θα δούμε τους τρόπους που μπορεί να γίνει αυτό:

- Όποτε ένα σήμα RTS (Request To Send) παραλαμβάνεται, ένα σήμα που συγκρούεται με το σήμα CTS (Clear To Send) διαβιβάζεται. Δεδομένου ότι οι κόμβοι δεν μπορούν να διαβιβάσουν τα στοιχεία πριν λάβουν το CTS, συνεχίζουν τα σήματα RTS.

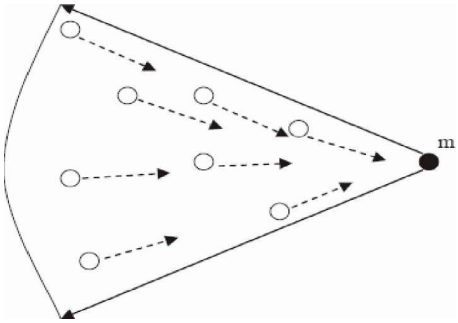
- Εάν το MAC είναι βασισμένο στις μη ενεργές και τις ενεργές περιόδους, η παρεμβολή των παρασίτων κατά την διάρκεια μόνο των ενεργών περιόδων μπορεί συνεχώς να εμποδίσει το κανάλι.
- Τα ψεύτικα σήματα RTS ή CTS με παραμέτρους τα δεδομένα μετάδοσης που στέλνονται συνεχώς, το οποίο κάνουν τους άλλους κόμβους που κάνουν την εικονική μεταφορά να περιμένουν για πάντα.
- Η εξαπάτηση της βεβαίωση λήψης, όπου ένας αντίπαλος στέλνει τις ψεύτικες βεβαιώσεις λήψης του στρώματος συνδέσεων για τα πακέτα που έχει κρυφακούσει και που απευθύνονται στους γειτονικούς κόμβους, μπορεί επίσης να είναι μια αποτελεσματική επίθεση DoS στρώματος συνδέσεων. Οι πιο σύνθετες επιθέσεις DoS μπορούν να σχεδιαστούν βασισμένες στο στρώμα της MAC. Παραδείγματος χάριν, στα δίκτυα αισθητήρων, τα πλήρη συστήματα διεύθυνσης δεν χρησιμοποιούνται. Αντ' αυτού, τα θέματα όπως η στοιχείο-κεντρική δρομολόγηση και η επαναχρησιμοποίηση διευθύνσεων μπορούν να χρησιμοποιηθούν. Ένας κακόβουλος κόμβος μπορεί να διευθύνει μια επίθεση sybil στο στρώμα της MAC για να κάνει τους άλλους κόμβους στην περιοχή να υποθέσουν ότι όλες οι διαθέσιμες διευθύνσεις χρησιμοποιούνται. Αυτό αποτρέπει τους κόμβους από το να γνωρίζουν την ύπαρξη μέρος του δικτύου.[10]

Γ) DoS against Routing Schemes

Τα μη δομημένα Ad Hoc δίκτυα έχουν ειδικές προκλήσεις δρομολόγησης, οι οποίες αντέχουν τους νέους τύπους επιθέσεων DoS ενάντια στα πρωτόκολλα του στρώματος δικτύου. Αυτές οι επιθέσεις εμπίπτουν γενικά σε μια από τις δύο κατηγορίες (Hu et al, 2005): επιθέσεις διάσπασης δρομολόγησης ή επιθέσεις κατανάλωσης των πόρων. Οι επιθέσεις διάσπασης δρομολόγησης στοχεύουν στη δυσλειτουργία της δρομολόγησης, που καθιστά το δίκτυο ανίκανο να παρέχει τις απαραίτητες υπηρεσίες δικτύωσης. Ο στόχος των επιθέσεων κατανάλωσης των πόρων είναι να καταναλωθούν οι πόροι δικτύων όπως το εύρος ζώνης, η μνήμη, η υπολογιστικές δύναμη και η ενέργεια. Και οι δύο είναι επιθέσεις άρνησης υπηρεσιών και τα παραδείγματά τους παρατίθενται παρακάτω (Karlof και Wagner, 2003):

- **Εξαπατημένες ή αλλαγμένες πληροφορίες δρομολόγησης:** οι πληροφορίες δρομολόγησης που ανταλλάσσονται μεταξύ των κόμβων μπορούν από τους κακόβουλους κόμβους να αλλάξουν για να έχουν μια καταστρεπτική επίδραση στο σχέδιο δρομολόγησης.
- **Επίθεση πλημμυρών** (Karlof και Wagner, 2003): ένας κακόβουλος κόμβος μπορεί να μεταδώσει σε όλους τους κόμβους του δικτύου πληροφορίες

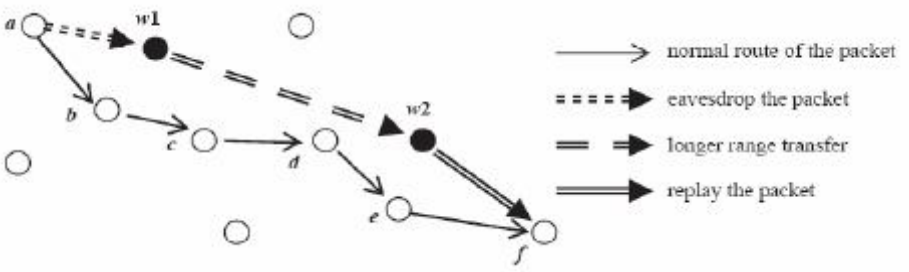
δρομολόγησης ή οποιεσδήποτε άλλες πληροφορίες με αρκετά υψηλό ρυθμό μετάδοσης έτσι ώστε να πειστεί κάθε κόμβος στο δίκτυο ότι είναι ο γείτονάς τους. Όταν οι άλλοι κόμβοι στέλνουν τα πακέτα τους στον κακόβουλο κόμβο, εκείνα τα πακέτα δεν παραλαμβάνονται από οποιοδήποτε άλλο κόμβο (σχήμα 22).



Εικόνα 22.*Επίθεση Πλημμύρας (Flooding Attack)*

- **Επίθεση Wormhole:** ένας κακόβουλος κόμβος μπορεί να λάβει πακέτα σε ένα σημείο και να τα μεταφέρει σε έναν άλλο κακόβουλο κόμβο, που είναι σε ένα άλλο μέρος του δικτύου, εκτός ζώνης καναλιού. Ο δεύτερος κακόβουλος κόμβος επαναλαμβάνει έπειτα τα πακέτα. Αυτό κάνει όλους τους κόμβους που μπορούν να ακούσουν τις μεταδόσεις του δεύτερο κακόβουλο κόμβο να θεωρούν ότι ο κόμβος που έστειλε τα πακέτα στον πρώτο κακόβουλο κόμβο είναι ο γείτονας τους και για το λόγο αυτό λαμβάνουν τα πακέτα άμεσα από αυτόν. Παραδείγματος χάριν, τα πακέτα που στέλνονται από τον κόμβο α (σχήμα 7) παραλαμβάνονται επίσης από τον κόμβο w1, ο οποίος είναι ένας κακόβουλος. Κατόπιν ο κόμβος w1 διαβιβάζει αυτά τα πακέτα στον κόμβο w2 μέσω ενός καναλιού που είναι εκτός της ζώνη για όλους τους υπόλοιπους κόμβους στο δίκτυο εκτός από τους αντιπάλους. Ο κόμβος w2 επαναλαμβάνει τα πακέτα και ο κόμβος φ τα λαμβάνει σαν τα ελάμβανε άμεσα από τον κόμβο α. Τα πακέτα που ακολουθούν την κανονική διαδρομή, δηλ. το α-β-γ-δ-ε- φ, φτάνουν στον κόμβο φ αργότερα από εκείνα που μεταβιβάστηκαν μέσω του wormhole και επομένως πέφτουν επειδή κάνουν περισσότερα βήματα. Τα Wormholes είναι πολύ δύσκολο να ανιχνευτούν και μπορούν να επηρεάσουν την απόδοση πολλών υπηρεσιών δικτύων όπως ο χρονικός συγχρονισμός, ο εντοπισμός και η μεταφορά δεδομένων.
- **Επίθεση αλλαγής δρομολόγησης:** ένας επιτιθέμενος μπορεί να προσπαθήσει την αλλαγή της κυκλοφορίας σε μια υποτιθέμενη διαδρομή ή να χωρίσει το δίκτυο. Διάφορες τεχνικές μπορούν να χρησιμοποιηθούν για αυτό. Παραδείγματος χάριν, ο Hu et al. (2005) καθόρισε μια τέτοια επίθεση, όπου ένας κόμβος σε μια διαδρομή προσθέτει εικονικούς κόμβους στη διαδρομή έτσι ώστε η διαδρομή να γίνεται δαπανηρότερη έναντι μιας άλλης διαδρομής.
- **Επιθέσεις sink hole:** ένας κακόβουλος κόμβος μπορεί να γίνει πολύ ελκυστικός στους περιβάλλοντες κόμβους όσον αφορά τον αλγόριθμο δρομολόγησης. Παραδείγματος χάριν, οι διαφημίσεις δρομολόγησης μπορούν να μεταδίδονται προς όλους και όλοι οι γειτονικοί κόμβοι μπορούν

να πειστούν ότι ο κακόβουλος κόμβος είναι ο καλύτερος επόμενος δρόμος για την αποστολή των πακέτων στο σταθμό βάσεων. Όταν ένας κόμβος γίνεται μια sink hole, γίνεται hub για την εγγύτητά της και αρχίζει να λαμβάνει όλα τα πακέτα που πηγαίνουν στο σταθμό βάσεων.



Εικόνα 23.*Επίθεση Wormhole*

- **Επίθεση μαύρων τρυπών (Blackhole attack):** ένας κακόβουλος κόμβος μπορεί να απορρίψει όλα τα πακέτα που λαμβάνει για αποστολή. Αυτή η επίθεση είναι ιδιαίτερα αποτελεσματική όταν ο επιτιθέμενος κόμβος είναι επίσης μια sink hole. Ένας τέτοιος συνδυασμός επίθεσης μπορεί να σταματήσει όλη την κυκλοφορία δεδομένων γύρω από τη μαύρη τρύπα.

- **Επιλεκτική αποστολή (Greyhole attack):** όταν ένας κακόβουλος κόμβος απορρίπτει όλα τα πακέτα, αυτό μπορεί να ανιχνευθεί εύκολα από τους γείτονές του. Επομένως, μπορεί να απορρίψει μόνο τα επιλεγμένα πακέτα και να διαβιβάσει άλλα.

- **Επίθεση ανακύκλωσης δρομολόγησης (Routing Loop):** οι sink hole επιθέσεις μπορούν να χρησιμοποιηθούν για να δημιουργήσουν routing loops για να καταναλώσουν την ενέργεια και το εύρος ζώνης καθώς επίσης και να αλλάξουν τη δρομολόγηση.

- **Επίθεση Rushing** (Hu et al., 2005): ένας επιτιθέμενος διαδίδει τα μηνύματα αιτήματος και απάντησης διαδρομών γρήγορα σε όλο το δίκτυο. Αυτό καταστέλλει οποιαδήποτε πιο πρόσφατα νόμιμο μήνυμα αιτήματος διαδρομών, δηλαδή οι κόμβοι τους απορρίπτουν, επειδή οι κόμβοι καταστέλλουν τα άλλα αντίγραφα ενός αιτήματος διαδρομών που έχουν επεξεργαστείήδη.

- **Επιθέσεις που εκμεταλλεύονται τους κόμβους τιμωρώντας τα συστήματα:** τα συστήματα που αποφεύγουν τους κόμβους χαμηλής απόδοσης μπορούν να χρησιμοποιηθούν από τους αντιπάλους. Παραδείγματος χάριν, οι κακόβουλοι κόμβοι μπορούν να εκθέσουν μηνύματα λάθους για έναν κόμβο που αποδίδει πραγματικά καλά. Επομένως, το σχέδιο δρομολόγησης μπορεί να αποφύγει μια διαδρομή που περιλαμβάνει αυτόν τον κόμβο. Ομοίως, μια σύνδεση μπορεί να φραχτεί για μια σύντομη περίοδο αλλά δεδομένου ότι τα μηνύματα λάθους παράγονται για τη σύνδεση κατά τη διάρκεια εκείνου του χρονικού διαστήματος, το σχέδιο δρομολόγησης μπορεί να συνεχίσει να αποφεύγει τη σύνδεση ακόμα κι αν δεν είναι φραγμένο άλλο.[11][12]

Δ) DoS in the Transport Layer

Τα πρωτόκολλα στρώματος μεταφοράς είναι επίσης ευαίσθητα στις απειλές ασφάλειας. Μερικά σενάρια επίθεσης εφαρμόσιμα σε αυτό το στρώμα παρατίθενται παρακάτω:

- **Επανάληψη του acknowledgement:** σε μερικά πρωτόκολλα στρώματος μεταφορών, όπως το TCP-Reno, αναγνωρίζοντας το ίδιο τμήμα πολλαπλές φορές στο δίκτυο δείχνει αρνητικό acknowledgement. Ένας κακόβουλος κόμβος μπορεί να επαναλάβει πολλαπλά ένα acknowledgement ώστε να γίνει ο κόμβος πηγής και να θεωρηθεί ότι το μήνυμα δεν παραδόθηκε επιτυχώς.
- **Jamming acknowledgements:** ένας κακόβουλος κόμβος μπορεί να φράξει τα τμήματα που μεταβιβάζουν τα acknowledgement. Αυτό μπορεί να οδηγήσει στη λήξη μιας σύνδεσης.
- **Μεταβαλλόμενος αριθμός ακολουθίας:** στα πρωτόκολλα όπως RMST και PSFQ, ένας κακόβουλος κόμβος μπορεί να αλλάξει τον αριθμό ακολουθίας ενός τεμαχίου και να κάνει τον παραλήπτη να θεωρήσει ότι μερικά πακέτα έχουν χαθεί.
- **Αίτημα spoofing σύνδεσης:** ένας κακόβουλος κόμβος μπορεί να στείλει πολλά αιτήματα σύνδεσης σε έναν κόμβο, καταναλώνοντας τους πόρους του έτσι ώστε δεν μπορεί να δεχτεί οποιοδήποτε άλλο αίτημα σύνδεσης.

Αυτός ο κατάλογος σεναρίων δεν είναι πλήρης. Πολλές διαφορετικές τακτικές μπορούν να αναπτυχθούν βασισμένες στο πρωτόκολλο που χρησιμοποιείται στο στρώμα μεταφορών.[12]

Misbehaving

Οι επιθέσεις DoS μπορούν μερικές φορές να προέλθουν από τους κόμβους μέσα στο δίκτυο. Μερικοί κόμβοι μπορούν να συμπεριφερθούν απρεπώς για να κερδίσουν κάποιους εκ των περιορισμένων πόρων της δικτύωσης, δηλαδή μπορούν να φερθούν εγωιστικά. Παραδείγματος χάριν, με τη χρησιμοποίηση του σχεδίου της MAC, ένας κόμβος άπρεπης συμπεριφοράς μπορεί να αναγκάσει τους άλλους κόμβους να περιμένουν περισσότερο έτσι ώστε να μείνουν ελεύθεροι πόροι του συστήματος για δικιά του χρήση. Οι κόμβοι μπορούν επίσης να είναι εγωιστικοί με την άρνηση να αναμεταδώσουν άλλα μηνύματα. Εάν κάθε κόμβος ενεργεί όπως αυτό, κατόπιν ο εγωισμός μπορεί να ασκήσει επίδραση παρόμοια με μια επίθεση DoS.

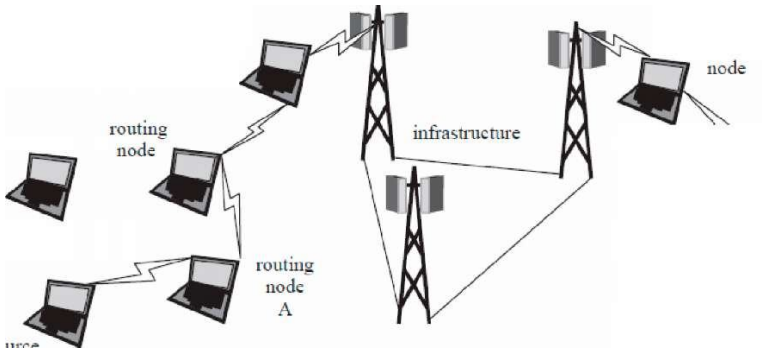
Ένας άλλος σκοπός της συμπεριφοράς αυτής μπορεί να στοχεύσει σε ένα σχέδιο χρέωσης με την άρνηση της πληρωμής για τις λαμβανόμενες υπηρεσίες. Καταρχάς τα ad hoc δίκτυα μπορούν να θεωρηθούν ως περιβάλλοντα όπου κάθε κόμβος συνεργάζεται ώστε να επικοινωνήσει με τον άλλον μέσω ενός ελεύθερου καναλιού. Αυτό όμως δεν συμβαίνει πάντα. Τα δίκτυα πλέγματος (mesh networks) παρέχουν την ασύρματη πρόσβαση multihop στις ευρυζωνικές υπηρεσίες. Ομοίως, μπορούν να υπάρξουν multihop στα κυψελοειδή δίκτυα όπου οι κόμβοι τους επιτρέπεται να έχουν πρόσβαση στο δίκτυο μέσω των ειδικών ασύρματων συνδέσεων multihop όταν είναι εκτός της περιοχή κάλυψης που παρέχεται από την υποδομή, όπως φαίνεται στο σχήμα 8. Στις δύο περιπτώσεις αυτές οι κόμβοι φθάνουν σε έναν φορέα παροχής υπηρεσιών και υποτίθεται ότι πρέπει να πληρώσουν για τις υπηρεσίες που παίρνουν από τον φορέα παροχής

υπηρεσιών (Salem et al. 2003). Οι διάφορες επιθέσεις που προβλέπονται ενάντια στα σχέδια χρέωσης σε αυτά τα είδη δικτύου είναι:

- **Refusal to pay:** ο κόμβος της πηγής μπορεί να αρνηθεί ότι πραγματοποίησε κάποια επικοινωνία σχετικά με ένα λογαριασμό.

- **Ανέντιμες ανταμοιβές (Dishonest rewards):** στη δικτύωση multihop, οι ενδιάμεσοι κόμβοι πρέπει να αναμεταδώσουν τα άλλα πακέτα. Αυτό μπορεί να γίνει παρακινώντας τους ενδιάμεσους κόμβους να διαβιβάσουν τα πακέτα αντί να είναι εγωιστικοί, σχεδιάζοντας μηχανισμούς ανταμοιβής. Σε αυτήν την περίπτωση, ένας κόμβος άπρεπης συμπεριφοράς μπορεί να θελήσει να εμφανιστεί ότι περιλήφθηκε στην αποστολή μερικών πακέτων, ακόμα κι αν δεν ήταν.

Ελεύθερη οδήγηση (Free riding): οι ενδιάμεσοι κόμβοι ανάμεσα στη διαδρομή μεταξύ της πηγής και του προορισμού μπορούν να τοποθετήσουν τα πακέτα τους προς τις τρέχουσες επικοινωνίες για να αποφύγουν το λογαριασμό. Παραδείγματος χάριν, ο κόμβος δρομολόγησης A μπορεί να τοποθετήσει το πακέτο του επάνω στα πακέτα του κόμβου δρομολόγησης B προκειμένου να πάει στον προορισμό του (Σχήμα 8)



Εικόνα 24.*Multihop cellular network*

ΚΕΦΑΛΑΙΟ 6^{Ο}

6.1 Αντιμετώπιση Επιθέσεων

Η ασφαλής δρομολόγηση (routing) είναι απαραίτητη για την αποδοχή και χρήση των Ad – Hoc δικτύων για πολλές εφαρμογές, αλλά τα τωρινά προτεινόμενα πρωτόκολλα δρομολόγησης ,για αυτά τα δίκτυα, είναι ανασφαλή. Ο σχεδιασμός ενός πρωτόκολλου δρομολόγησης το οποίο να ικανοποιεί τους προτεινόμενους στόχους ασφαλείας είναι ένα ανοιχτό πρόβλημα. Η κωδικοποίηση ζεύξης στρώματος και οι μηχανισμοί αυθεντικότητας μπορεί να είναι μια πρώτη λογική προσέγγιση για άμυνα από mote-class insiders, άλλα η κρυπτογράφηση, από μόνη της, δεν είναι αρκετή. Η

πιθανή παρουσία εχθρών με lap-top, insiders και η περιορισμένη συσχέτιση μηχανισμών ασφαλείας end-to-end απαιτούν προσεκτικό σχεδιασμό πρωτοκόλλων.

6.2 Συστήματα Ανίχνευσης Επιθέσεων (IDS)

Τα συστήματα ανίχνευσης επιθέσεων (Intrusion Detection Systems), αν και δεν είναι καινούργια, τα τελευταία χρόνια άρχισαν να εφαρμόζονται στα Ad - Hoc δίκτυα. Τα συστήματα ανίχνευσης απειλών είναι προϊόντα με μορφή λογισμικού ή και υλικού, τα οποία αυτοματοποιούν τη διαδικασία ελέγχου, ανάλυσης, αναγνώρισης και αντίδρασης σε παράνομες δραστηριότητες. Τα συστήματα αυτά συλλέγουν πληροφορίες και στη συνέχεια τις αναλύουν για ενδείξεις εισβολής, προβαίνοντας σε κατάλληλες ενέργειες αντιμετώπισης. Όταν το σύστημα ανίχνευσης εισβολών συλλέγει πληροφορίες για το δίκτυο και προσπαθεί να αποφανθεί για το αν δέχεται επίθεση ή όχι, τότε έχουμε «δικτυακό σύστημα ανίχνευσης εισβολής» (Network Based IDS). Ενώ όταν συλλέγονται και επεξεργάζονται πληροφορίες σε επίπεδο υπολογιστή - διακομιστή για να αποφασίσει αν το σύστημα δέχεται επίθεση, τότε έχουμε «σύστημα ανίχνευσης εισβολής εγκατεστημένο σε υπολογιστή» (Host Based IDS).[10]

6.3 Πλαίσιο Λειτουργίας IDS Συστημάτων

Η ομαλή λειτουργία ενός δικτύου θέτει τα πλαίσια δραστηριοτήτων των Σ.Α.Ε.. Απαραίτητη προϋπόθεση για την σωστή λειτουργία ενός Σ.Α.Ε. είναι η τήρηση συγκεκριμένων χαρακτηριστικών από το δίκτυο. Γενικά χαρακτηριστικά:

- Οι ενέργειες των κόμβων και οι διεργασίες που εκτελούνται από δίκτυο θα πρέπει να ακολουθούν έναν στατιστικά προβλέψιμο πρότυπο.

- Οι ενέργειες των κόμβων δεν θα πρέπει σε καμία περίπτωση να υπονομεύουν την πολιτική ασφαλείας του δικτύου.

- Κάθε ομάδα κόμβων χρησιμοποιεί συγκεκριμένο σύνολο εντολών εντός των επιτρεπτών ορίων. Ένα παράδειγμα από την καθημερινή ζωή για την συγκεκριμένη περίπτωση, θα μπορούσε π.χ. να αποτελεί το γεγονός, ένας πελάτης να εισάγει εντολές συντήρησης ενός συστήματος.

Αν το δίκτυο δέχεται επίθεση, τότε κάποιο από τα παραπάνω χαρακτηριστικά δεν τηρείται. Τα Σ.Α.Ε. στηρίζουν την επιτήρηση τους στη πληρότητα των χαρακτηριστικών αυτών. Συνεπώς τα παραπάνω, γενικά χαρακτηριστικά, είναι προαπαιτούμενα για την ομαλή λειτουργία ενός Σ.Α.Ε..

6.4 Γενικά Χαρακτηριστικά IDS

Κάθε τύπος συστήματος ανίχνευσης εισβολών έχει ένα συγκεκριμένο τρόπο λειτουργίας. Το σύστημα αποτελείται από διαφορετικά αλληλοσυνδεόμενα μέρη. Κάθε ένα από αυτό έχει επωμιστεί με τη διεκπεραίωση κάποιας υπηρεσίας. Ένα τυπικό IDS περιλαμβάνει τα ακόλουθα:

- Μηχανισμό συλλογής πρωτογενούς πληροφορίας. Στόχος του είναι η σύλληψη των συμβάντων και η συλλογή των πληροφοριών σχετικά με αυτά. Σε ένα δίκτυο η αποστολή δεδομένων από ένα κόμβο, αποτελεί ένα συμβάν και τα δεδομένα την πληροφορία του συμβάντος.

- Μηχανισμό επεξεργασίας των πληροφοριών. Η επεξεργασία των πληροφοριών είναι το πιο νευραλγικό τμήμα διότι αναλύει διεξοδικά τα στοιχεία που συλλέχθηκαν από το προηγούμενο τμήμα και λαμβάνει την απόφαση για την λήψη δράσης ή όχι.

- Μηχανισμό αντίμετρων. Ο μηχανισμός αυτός αναπτύσσεται σε περίπτωση αναγνώρισης εισβολής. Ειδοποιεί το αρμόδιο προσωπικό ή αυτοματοποιημένα λαμβάνει δράση έναντι του επιτιθέμενου.

- Μηχανισμό αποθήκευσης και ανάκλησης των πληροφοριών. Η αποθήκευση των πληροφοριών και των αντίμετρων που πιθανώς αναπτύχθηκαν εξυπηρετεί σκοπούς διατήρησης αρχείου. ' Αποθηκεύονται σε βάσεις δεδομένων ή σε αρχεία τύπου ημερολογίου για περαιτέρω χρήση ή ανάλυση. Ουσιαστικά αποτελούν το ιστορικό του συστήματος.

Το ιδανικό σύστημα ανίχνευσης επίθεσης θα πρέπει να καλύπτει συγκεκριμένα κριτήρια. Για να επιτευχθεί ο μέγιστος βαθμός προστασίας και ευελιξίας ενός IDS απαιτείται, κατά τη φάση της ανάπτυξης του, να λαμβάνονται υπόψη τα παρακάτω χαρακτηριστικά στοιχεία:

- Το IDS θα πρέπει να έχει μεγάλο εύρος ανίχνευσης απειλών. Αν αυτό δεν είναι εφικτό κατά τα πρώτα στάδια ανάπτυξης του, μπορεί να ενσωματωθεί μηχανισμός εκμάθησης. Είναι σπουδαίο πλεονέκτημα το IDS να έχει τη δυνατότητα προσαρμογής σε νέες απειλές ή αλλαγές της συμπεριφοράς των κόμβων

- Επίσης, θα πρέπει να ανιχνεύει έγκαιρα τις επιθέσεις. Διακρίνονται δύο κατηγορίες IDS. Η πρώτη λειτουργεί off - line και συνεπώς μπορεί να ενημερώσει για επίθεση μόνο αφού έχει ήδη γίνει. Η δεύτερη λειτουργεί runtime έχοντας την δυνατότητα προειδοποίησης ακόμη και πριν εκδηλωθεί μία επίθεση. Περισσότερες λεπτομέρειες θα δοθούν παρακάτω.

- Πρέπει να έχει όσο το δυνατό λιγότερους εσφαλμένους συναγερμούς (false positive / negative alarm), δηλαδή ότι το δίκτυο δέχεται επίθεση, ενώ κάτι τέτοιο δεν συμβαίνει. Χαμηλός ρυθμός εσφαλμένων συναγερμών συνιστά ένα ακριβές σύστημα. Πρέπει να σημειωθεί ότι η ακρίβεια ενός IDS είναι πολλές φορές παραμετροποιήσιμη.

- Το IDS θα πρέπει να έχει τη δυνατότητα να διαχειρίζεται αυτόνομα τα σφάλματα του. Όπως κάθε λογισμικό έτσι και σε αυτή τη περίπτωση

επιβάλλεται η ορθή αντιμετώπιση των σφαλμάτων. Τη στιγμή που θα παρουσιάσει σφάλμα το σύστημα θα πρέπει να διακοπεί οποιαδήποτε συναλλαγή στο δίκτυο και στη συνέχεια να επανέρχεται χωρίς ανθρώπινη παρέμβαση στη κατάσταση που ήταν πριν αυτό.

- Όσο είναι δυνατό θα πρέπει να είναι ανεξάρτητο πλατφόρμας (cross compatibility).

- Τέλος, το IDS θα πρέπει να εκτελείται καταναλώνοντας όσο το δυνατό λιγότερους πόρους συστήματος. Ιδιαίτερα σοβαρό θέμα, καθώς η συνεχής λειτουργία του παράλληλα με του δικτύου, χωρίς σωστή διαχείριση πόρων, μπορεί να προκαλέσει κατάρρευση του ίδιου του δικτύου.[10]

6.5 Ταξηνόμηση IDS

Τα συστήματα ανίχνευσης επίθεσης δύναται να ταξινομηθούν με βάση το μοντέλο συμπεριφοράς που ακολουθούν.
Ως μοντέλο συμπεριφοράς ορίζεται το πρότυπο του τυπικού κόμβου του δικτύου που προστατεύουν. Τα IDS χρησιμοποιούν μοντέλα συμπεριφοράς για την «μέτρηση» της απόκλισης της παρατηρούμενης συμπεριφοράς με την καταχωρημένη. Αυτά τα συστήματα καλούνται μοντέλα ανίχνευσης διαταραχών (anomaly detection).
Το άλλο είδος IDS χρησιμοποιεί μοντέλα συμπεριφοράς για τη σύγκριση των καταγραφόμενων ενεργειών ενός κόμβου με καταχωρημένες υπογραφές γνωστών απειλών. Αυτά ονομάζονται μοντέλα κακής συμπεριφοράς (misuse detection / signature detection). Στην πράξη τα προαναφερθέντα μοντέλα συνδυάζονται συχνά μεταξύ τους.

6.6 Μοντέλα ανίχνευσης Διαταραχών

Τα μοντέλα ανίχνευσης διαταραχών θεωρούν ότι η απροσδόκητη συμπεριφορά αποτελεί τεκμήριο επίθεσης. Η λήψη απόφασης γίνεται με στατιστική επεξεργασία των ενεργειών των κόμβων.

Μία υποκατηγορία αυτών των μοντέλων, είναι τα μοντέλα κατωφλίου (threshold detection). Αυτού του είδους τα μοντέλα λαμβάνουν απόφαση για τη λήψη μέτρων με βάση κάποιες προκαθορισμένες τιμές κατωφλίου. Στην εμφάνιση ενός αναμενόμενου γεγονότος αποδίδεται ένα όριο τιμών, αν το γεγονός συμβεί με τιμή εκτός ορίων τότε σημάνει συναγερμός. Αυτό βοηθά στην εύκολη παραμετροποίηση, ενώ αυξάνει την πολυπλοκότητα του μοντέλου.

Μία ακόμα υποκατηγορία είναι τα μοντέλα στατιστικών ροπών. Το μοντέλο αυτό χρησιμοποιεί στατιστικές ροπές. Ο αναλυτής γνωρίζει τον μέσο και την τυπική απόκλιση (οι δύο πρώτες ροπές) και πιθανότατα άλλα μέτρα συσχέτισης (ροπές υψηλότερης τάξης). Αν οι τιμές βρίσκονται εκτός του αναμενόμενου διαστήματος γι' αυτή τη ροπή, η συμπεριφορά που αντιπροσωπεύουν οι τιμές θεωρείται διαταραγμένη. Επειδή η κατανομή της περιγραφής του συστήματος μπορεί να εμπεριέχει καθυστερήσεις, τα μοντέλα ανίχνευσης διαταραχών συνυπολογίζουν αυτές τις αλλαγές τροποποιώντας τους στατιστικούς κανόνες με βάση τους οποίους λαμβάνονται οι αποφάσεις. Επιπλέον η

περιγραφή της κατανομής κάθε συστήματος ενημερώνεται σε τακτά χρονικά διαστήματα (π.χ. κάθε μέρα), με βάση τη συμπεριφορά που έχει παρατηρηθεί. Τα μοντέλα στατιστικών ροπών παρέχουν μεγαλύτερη ευελιξία από τα μοντέλα τιμών κατωφλίου. Με την ευελιξία, όμως, εμφανίζονται και προβλήματα πολυπλοκότητας.

Η τρίτη υποκατηγορία είναι τα μοντέλα πρόβλεψης προτύπων. Αυτό το μοντέλο ανίχνευσης σκοπό έχει την πρόβλεψη μελλοντικών συμβάντων χρησιμοποιώντας τη γνώση συμβάντων που έχουν ήδη πραγματοποιηθεί. Κάθε συμβάν που έχει ήδη πραγματοποιηθεί, θέτει το σύστημα σε μία κατάσταση το αμέσως επόμενο συμβάν το θέτει σε μία άλλη κατάσταση, έτσι κατασκευάζεται ένα σύνολο πιθανοτήτων μετάβασης. Ένα συμβάν με χαμηλό ποσοστό εμφάνισης αποτελεί πιθανή απειλή. Το ακόλουθο παράδειγμα αποδεικνύει τον τρόπο λειτουργίας του συστήματος. Έστω ότι ισχύει ο κανόνας:

E1-E2 -> (E3 = 86%, E4 = 14%)

Αυτό σημαίνει ότι με γνωστή χρονική σειρά των καταστάσεων E1 και E2, η πιθανότητα να ακολουθήσει το E3 είναι 86% και το E4 14%. Συνεπώς αν μετά τα E1 και E2 ακολουθήσει το E5 θα σημάνει συναγερμός (δεν αναμένονταν η εμφάνιση του). Το πρόβλημα προκύπτει όταν το E5 είναι εντελώς άγνωστο, τότε μπορεί απλά να χαρακτηρισθεί ως ύποπτο, όμως κάτι τέτοιο αυξάνει τους εσφαλμένους συναγερμούς. Γενικά, τα μοντέλα πρόβλεψης προτύπων ανιχνεύουν ανώμαλες συμπεριφορές ευκολότερα από τα άλλα μοντέλα, είναι πιο προσαρμόσιμα σε αλλαγές και απαιτούν μικρό χρόνο εκτέλεσης.

6.7 Μοντέλα Ανίχνευσης Κακής Συμπεριφοράς

Η ανίχνευση κακής συμπεριφοράς (misuse detection) βασίζεται στην αναζήτηση καταστάσεων του συστήματος που είναι γνωστό ότι είναι βλαβερές. Ο τρόπος λειτουργίας των μοντέλων μοιάζει με την λειτουργία των αντιβιοτικών λογισμικών. Μπορούν να ανιχνεύσουν όλες τις γνωστές επιθέσεις αλλά το κύριο μειονέκτημα τους είναι η αδυναμία να αντιμετωπίσουν άγνωστες απειλές. Είναι αρκετά σοβαρό πρόβλημα διότι η ταυτοποίησης μίας απειλής προϋποθέτει την επιτυχή εκτέλεση της τουλάχιστον μία φορά. Παράλληλα, οι διαχειριστές καλούνται συνεχώς να ενημερώνουν τους κανόνες κακής συμπεριφοράς. Από την άλλη, το πλεονέκτημα τους είναι ότι όταν αντιληφθούν μία συγκεκριμένη απειλή έχουν την δυνατότητα να παρέχουν πολλές πληροφορίες σχετικά με αυτή.

6.8 Αντιμετώπιση Απειλών

Τα συστήματα ανίχνευσης απειλών ενσωματώνουν μηχανισμούς ανάπτυξης αντίμετρων έναντι των επιθέσεων. Στόχος είναι να αντιμετωπισθεί η απειλή και να προστατευθεί το δίκτυο. Ορισμένα συστήματα αποτρέπουν την επίθεση, ενώ κάποια άλλα αποκρίνονται στην επίθεση και καταβάλλουν προσπάθεια να αποκαταστήσουν την εφαρμογή.

Το βέλτιστο θα ήταν η ανίχνευση και διακοπή της απόπειρας εισβολής προτού καταστεί επιβλαβής. Αυτό απαιτεί την συνεχή λειτουργία του συστήματος και την τοποθέτηση του στην πρώτη γραμμή άμυνας. Αναλυτικότερα, είναι προτιμότερο κάθε είσοδος πριν εισαχθεί στο δίκτυο, πρώτα να ελέγχεται από το IDS, προλαμβάνοντας κατά αυτό τον

τρόπο την επίθεση. Ακόμη καλύτερα αν το IDS λειτουργεί ως μηχανισμός του ίδιου του πρωτοκόλλου δρομολόγησης και όχι ανεξάρτητα, δίνεται η εντύπωση στους επιτιθέμενους ότι η επίθεση πέτυχε.

Συνεπώς τα IDS εφαρμόζουν διαφορετικά αντίμετρα κατά περίπτωση. Οι δυνατές ανταποκρίσεις ενός συστήματος είναι οι ακόλουθες:

- Καταστολή της επίθεσης με ταυτόχρονη απομάκρυνση του επιτιθέμενου από το δίκτυο. Πλήρης απόρριψη του κακόβουλου κόμβου και περιορισμός του σε ελεγχόμενη περιοχή.
- Ταυτοποίηση μίας επίθεσης και κατάταξης της ως προς το είδος και την επικινδυνότητα της.
- Περιορισμός της ζημιάς περιορίζοντας τον κακόβουλο κόμβο.
- Αποκατάσταση του δικτύου.
- Παρακολούθηση της επίθεσης συλλέγοντας πληροφορίες για το προφίλ του επιτιθέμενου.
- Η αντεπίθεση δεν θα πρέπει να βασίζεται σε έναν αυτοματοποιημένο μηχανισμό.

6.9 Ισορροπία Κατανάλωσης Ισχύος

Οι τεχνικές αυτές θα είναι εφαρμόσιμες όπου είναι δυνατόν. Όποτε μια λειτουργία εκτελείται στο hardware, μια συμπληρωματική λειτουργία θα πρέπει να εκτελείται για να διαβεβαιώσει ότι η συνολική κατανάλωση ισχύος της μονάδας διατηρεί ισορροπία σχετικά με τις ψηλές τιμές.

Τέτοια σχετική λειτουργία με την οποία η κατανάλωση ισχύος είναι σταθερή και ανεξάρτητη από τις εισόδους και τα bits κλειδιών, εμποδίζει όλα τα είδη των επιθέσεων κατανάλωσης ισχύος

6.10 Μείωση του Μεγέθους του Σήματος

Μια προσέγγιση για την αποτροπή επιθέσεων DPA (Differential Power Analysis) είναι η μείωση των μεγεθών σημάτων, όπως η χρησιμοποίηση ενός σταθερού μονοπατιού εκτέλεσης κώδικα, και ισορροπώντας βάρη Hanging και να αναφέρουν μεταβάσεις ή να προασπίζουν φυσικώς την συσκευή. Δυστυχώς, τέτοια μείωση μεγέθους σήματος γενικά, δεν μειώνει το μέγεθος του σήματος στο μηδέν, όπως ένας εισβολέας με έναν άπειρο αριθμό δειγμάτων, που είναι ικανός να εκτελέσει DPA στο (υψηλά διαβαθμισμένο) σήμα.

6.11 Πρόσθεση Θορύβου

Άλλη μια προσέγγιση εναντίον του DPA είναι η εισαγωγή θορύβου μέσα στα μέτρα για την κατανάλωση ισχύος.

Όπως οι μειώσεις μεγέθους σήματος, έτσι και η πρόσθεση θορύβου αυξάνει τον αριθμό των απαιτούμενων δειγμάτων για την επίθεση, πιθανώς σε ένα μεγάλο αριθμό. Εξάλλου, η εκτέλεση χρονισμού και η τάξη μπορεί να υποτίθεται ότι παράγει ένα παρόμοιο αποτέλεσμα. Ξανά, μόνος του ο χρόνος αυξάνει τον αριθμό των δειγμάτων που απαιτούνται, παρόλα αυτά εάν αυτός αυξάνεται, είναι αρκετά μεγάλος για να κάνει την δειγματοληψία ακατόρθωτη, εξαιτίας του απαιτούμενου αριθμού δειγμάτων, οπότε το μέτρο αντιμετώπισης λειτουργεί κανονικά

Μια επίλυση του προβλήματος για να αποφευχθούν επιθέσεις DPA χρησιμοποιώντας τον θόρυβο, είναι η πρόσθεση τυχαίων υπολογισμών που αυξάνουν το επίπεδο θορύβου αρκετά, για να κάνει τα σημεία κλίσης DPA (DPA bias spikes) μη ανιχνεύσιμα. Ο κύριος στόχος είναι να προστεθεί αρκετός τυχαίος θόρυβος για να σταματήσει μια επίθεση, και όχι μόνο να προσθέσει μια minimal επικεφαλίδα.

6.12 Τροποποίηση του Σχεδιασμού Αλγορίθμου

Μια τελευταία προσέγγιση εναντίον των επιθέσεων του DPA είναι ο σχεδιασμός κρυπτοσυστημάτων με ρεαλιστικές υποθέσεις για το επικείμενο (underlying) hardware. Σαν απλό παράδειγμα, hashing ένα 160 bito κλειδί με το SHA πριν την χρησιμοποίηση του σαν κλειδί θα μπορούσε αποτελεσματικά να καταστρέψει μερικές πληροφορίες που πιθανόν ένας εισβολέας να έχει μαζέψει για το κλειδί. Ομοίως, η χρήση του δείκτη και της τροποποίησης του προτύπου (modulus) των επεξεργαστών σε κοινό κλειδί σχεδίων μπορεί να χρησιμοποιηθεί για να εμποδίσει τους εισβολείς από μια συσσώρευση πληροφοριών μέσα από έναν μεγάλο αριθμό λειτουργιών.

Αυτό μπορεί να λύσει το πρόβλημα, αλλά απαιτεί αλλαγές σχεδιασμού στους αλγόριθμους και στα ίδια τα πρωτόκολλα τα οποία είναι δυνατόν να κάνουν το αποτελεσματικό προϊόν να μη ενδίδει με τα στάνταρ και τις λεπτομέρειες.

6.13 Ανίχνευση Επιθέσεων

Η ανίχνευση μιας εξελισσόμενης επίθεσης άρνησης υπηρεσίας βασίζεται σε τεχνικές διάγνωσης ανωμαλίας. Πέρα από την καθ' αυτή ανακάλυψη μιας επίθεση DDoS η πρόκληση για έναν διαχειριστή ή ένα αυτόματο σύστημα IDS είναι να καταφέρουν να διαχωρίσουν περιστατικά φυσιολογικής αύξησης της κίνησης από πραγματικές κακόβουλες επιθέσεις. Μέρος της διαδικασίας ανίχνευσης είναι και ο προσδιορισμός των χαρακτηριστικών της κίνησης επίθεσης. Τα χαρακτηριστικά αυτά θα επιτρέψουν να διαχωριστεί από νόμιμες επικοινωνίες ή άλλες (ταυτόχρονες) επιθέσεις, και θα προσδιορίσουν τυχόν μέτρα αντιμετώπισης της. Η δυσκολία που παρουσιάζει το πρόβλημα της ανίχνευσης έγκειται, αφενός στην εξασφάλιση της απαραίτητης υπολογιστικής ισχύος ώστε να γίνει με επαρκή ταχύτητα η ανάλυση στοιχείων (ειδικά στα Ad - Hoc δίκτυα), αφετέρου στην εγκυρότητα και απόδοση των αλγορίθμων που θα χρησιμοποιηθούν για την ανάλυση.

Απ' ευθείας ανίχνευση γίνεται στο δίκτυο-θύμα με την παρατήρηση αυξημένης κίνησης ή και συμφόρησης. Για την ανακάλυψη ανωμαλιών στην κίνηση αυτή πρέπει να καταγραφεί, κατά τον ίδιο τρόπο που αυτό γίνεται στα συστήματα Network IDS (NIDS), και στη συνέχεια να αναλυθούν διάφορα χαρακτηριστικά της. Η μετρούμενη αύξηση της χρησιμοποίησης μιας σύνδεσης μεταξύ κόμβων, μπορεί να οφείλεται σε φυσιολογικά αίτια και επομένως απαιτείται ανάλυση του είδους και του προορισμού της.

Οι μέθοδοι που επιτρέπουν την καλύτερη διάκριση των αιτιών της συμφόρησης του δικτύου και, εφόσον ανιχνευτεί μια εξελισσόμενη επίδεση, εντοπίζουν τα χαρακτηριστικά της, βασίζονται στη λεπτομερή ανάλυση της εισερχόμενης κίνησης. Με βάση αυτές τις μετρήσεις ροών μπορούν να υλοποιηθούν συστήματα IDS διάγνωσης ανωμαλιών για περιστατικά DDoS. Αναλογικά μεγάλη αύξηση πακέτων σε σχέση με τις ροές κίνησης αποτελεί ένδειξη για την ύπαρξη μιας συνεχούς αποστολής δεδομένων από τις ίδιες πηγές προς τις ίδιες κατευθύνσεις. Δυσανάλογα πολλές ροές και αύξηση του λόγου ροών προς πακέτα, δείχνουν την αποστολή μικρού αριθμού πακέτων από μεγάλο αριθμό πολλών διαφορετικών διευθύνσεων. Οι παράμετροι αυτοί μπορούν να συνδυαστούν και με άλλα δεδομένα όπως το εύρος των διευθύνσεων παραλήπτη, τα συγκεκριμένα είδη των πακέτων κ.λπ. Τα στοιχεία αυτά μπορούν να διαγνώσουν κάποια περιστατικά DDoS ακόμα και αν η κίνηση δεν παρουσιάζει συνολικά σημαντικές διαφορές.

6.14 Ανακάλυψη της Διαδρομής

Η ανακάλυψη της διαδρομής που ακολουθεί μια επίδεση για να καταλήξει στο θύμα επιτρέπει, αν γίνει κατά τη διάρκεια ενός περιστατικού, την ανάσχεση της. Στην περίπτωση αυτή ο εντοπισμός του μονοπατιού θα πρέπει να γίνει πολύ σύντομα και με μεγάλη ακρίβεια. Ακόμα όμως και μετά από το τέλος του περιστατικού, η ανακάλυψη της πλήρους διαδρομής μπορεί να οδηγήσει στην πηγή της επίθεσης και να αποτρέψει την περαιτέρω δράση της. Αυτοματοποιημένες διαδικασίες ανακάλυψης της διαδρομής απαιτούν συνήθως να προϋπάρχουν κατάλληλες υποδομές ανίχνευσης και παρακολούθησης.

6.15 Αντίδραση στην Επίθεση

Διαδικασίες μη ορισμένες με σαφήνεια και μη αυτοματοποιημένες δεν παρέχουν την ταχύτητα που απαιτείται για το χειρισμό τέτοιων περιστατικών. Επιπλέον δεν υπάρχει τυποποίηση στα δεδομένα που θα ανταλλαγούν.

Ένας πρόσθετος παράγοντας δυσκολίας είναι η συνήθης έλλειψη συγκεκριμένης πολιτικής αντιμετώπισης των επιθέσεων.

Οι δυνατές λύσεις αντιμετώπισης των επιδέσεων DDoS μπορούν να κατηγοριοποιηδούν ως προληπτικές (proactive) ή κατασταλτικές (reactive).

- Μια πολύ τυπική προληπτική αντίδραση είναι η παρεμπόδιση πακέτων με διευθύνσεις προέλευσης που δεν αντιστοιχούν στις εφαρμοζόμενες πολιτικές δρομολόγησης. Προφανώς όσο μεγαλύτερος αριθμός κόμβων συμμετέχει, τόσο πιο αποδοτικό θα είναι το αποτέλεσμα κατά των επιδέσεων DDoS. Εντούτοις η μέθοδος έχει αδυναμίες: χρειάζεται αποδοτική υλοποίηση των αλγορίθμων φιλτραρίσματος, με δεδομένο ότι πρόκειται για κόμβους που χειρίζονται μεγάλους όγκους κίνησης. Επιπλέον υπάρχουν περιπτώσεις που η ακριβής δρομολόγηση δεν είναι γνωστή και έτσι η μέθοδος μπορεί να οδηγήσει σε παρεμπόδιση νόμιμων επικοινωνιών.

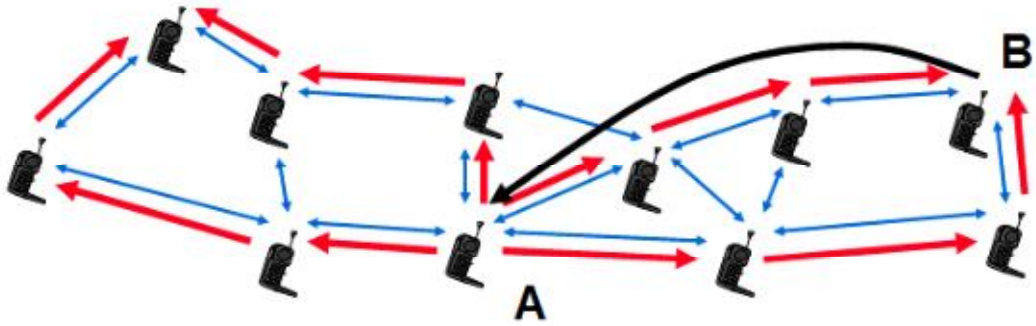
- Όταν η επίθεση έχει σα στόχο μόνον ένα συγκεκριμένο κόμβο, μια πρακτική που χρησιμοποιείται είναι η πλήρης διακοπή της κίνησης προς αυτόν στον ακριβώς προηγούμενο κόμβο. Η μέθοδος ονομάζεται «διοχέτευση σε μαύρη τρύπα» (blackholing) και μπορεί να υλοποιηθεί πολύ εύκολα. Επιπλέον δεν έχει ιδιαίτερο υπολογιστικό κόστος επειδή χρησιμοποιείται ο μηχανισμός

δρομολόγησης αντί αυτού του φιλτραρίσματος. Αν και ολοκληρώνει την άρνηση δικτυακής σύνδεσης προς το θύμα, ουσιαστικά αποκόπτοντάς το, το δίκτυο ανακουφίζεται από την κακόβουλη κίνηση.

- Μια άλλη πρόταση συνδυάζει την επιλογή νέας δρομολόγησης για την κίνηση του θύματος μέσα από σήραγγες με μια παραλλαγή της μεθόδου αποκοπής της επιθετικής κίνησης προς το τελικό θύμα. Στο δίκτυο δημιουργούνται σήραγγες. Στη συνέχεια όλη η κίνηση προς το θύμα οδηγείται από αυτό το δρόμο. Στη συνέχεια μέσα από άλλες σήραγγες η νόμιμη κίνηση καταλήγει στον παραλήπτη. Η λύση αυτή, απαιτεί τη γρήγορη ανίχνευση των επιθέσεων, την αλλαγή στη δρομολόγηση προς και από συγκεκριμένους κόμβους και, κυρίως, την ικανότητα για ακριβή εντοπισμό της κακόβουλης κίνησης προς και από το θύμα.[10][4]

ΚΕΦΑΛΑΙΟ 7ο

7.Ασφάλεια Δρομολόγησης

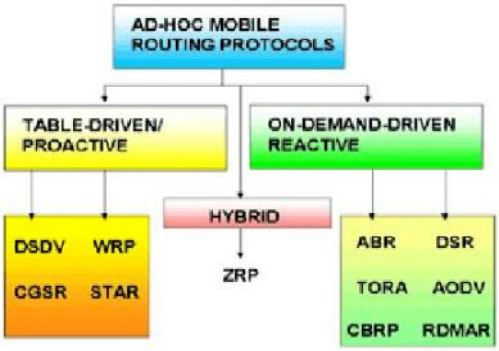


Εικόνα 25*Δρομολόγηση στα ad-hoc δίκτυα*

Ένα πρωτόκολλο δρομολόγησης ενός MANET βρίσκει διαδρομές ανάμεσα στους κόμβους στους οποίους προωθούνται τα πακέτα δεδομένων προς τον τελικό προορισμό. Σε αντίθεση με τα παραδοσιακά δίκτυα, τα πρωτόκολλα δρομολόγησης των MANETs πρέπει να είναι προσαρμόσιμα για να αντιμετωπίσουν τα χαρακτηριστικά που παρουσιάστηκαν παραπάνω και ιδιαίτερα τις συχνές αλλαγές στην τοπολογία του δικτύου. Το πρόβλημα-πρόκληση της δρομολόγησης των ad-hoc δικτύων έχει μελετηθεί εκτενώς, ιδιαίτερα από την ομάδα του MANET, την Internet Engineering Task Force (IETF). Αυτές οι μελέτες έχουν κατασταλάξει σε διάφορα πρωτόκολλα, τα οποία μπορούν να χωριστούν σε δύο κατηγορίες: proactive (table driven) και reactive (on-demand). Τα reactive πρωτόκολλα είναι πιο προσαρμόσιμα στα MANET περιβάλλοντα από ότι τα proactive. Η Εικόνα 26 δείχνει τις κατηγορίες των πρωτοκόλλων δρομολόγησης των ad-hoc δικτύων.

Εν τούτοις, το πρόβλημα με όλες αυτές τις λύσεις είναι ότι εμπιστεύονται όλους τους κόμβους και δε λογοδοτούν για την ασφάλεια, γι' αυτό είναι πολύ τρωτά σε επιθέσεις. Είναι πολύ σημαντικό να ασφαλίζουμε το πρωτόκολλο δρομολόγησης.

Αν το πρωτόκολλο δρομολόγησης υπονομεύεται (subverted) και τα μηνύματα μπορούν να μεταβάλλονται στη μεταφορά, τότε καμία ασφάλεια στα πακέτα δεδομένων των ανώτερων επιπέδων μπορεί να μετριάσει τις απειλές.



Εικόνα 26. *Οι κατηγορίες των πρωτοκόλλων δρομολόγησης των ad-hoc δικτύων*

Για την εξασφάλιση της διαθεσιμότητας, τα πρωτόκολλα δρομολόγησης πρέπει να είναι 'γερά' ενάντια στη δυναμικά μεταβαλλόμενη τοπολογία και τις κακόβουλες επιθέσεις. Τα πρωτόκολλα δρομολόγησης που προτείνονται για τα ad-hoc δίκτυα αντιμετωπίζουν καλά τη δυναμικά μεταβαλλόμενη τοπολογία. Εντούτοις, κανένα από τα γνωστά πρωτόκολλα δεν έχει προσαρμόσει μηχανισμούς που να υπερασπίζουν τα δίκτυα από τις κακόβουλες επιθέσεις. Για τα πρωτόκολλα δρομολόγησης των ad-hoc δικτύων γίνονται ακόμα έρευνες.

Δεν υπάρχει ακόμα ούτε ένα κατάλληλο πρωτόκολλο δρομολόγησης χωρίς ατέλειες. Επομένως, στόχος είναι η σύλληψη των κοινών απειλών ασφάλειας και η παροχή ασφάλειας στα πρωτόκολλα δρομολόγησης.

Στα περισσότερα πρωτόκολλα δρομολόγησης, οι δρομολογητές ανταλλάσσουν πληροφορίες για την τοπολογία του δικτύου προκειμένου να καθιερωθούν οι διαδρομές μεταξύ των σταθμών. Τέτοιες πληροφορίες θα μπορούσαν να γίνουν στόχος για τους κακόβουλους αντιπάλους που σκοπεύουν να κτυπήσουν το δίκτυο.

Υπάρχουν δύο πηγές απειλών στα πρωτόκολλα δρομολόγησης. Ο πρώτος προέρχεται από τους εξωτερικούς επιτιθεμένους. Με την διοχέτευση λανθασμένων πληροφοριών δρομολόγησης, επαναλαμβάνοντας παλιές πληροφορίες δρομολόγησης, ή διαστρεβλώνοντας τις πληροφορίες δρομολόγησης, ένας επιτιθέμενος θα μπορούσε επιτυχώς να χωρίσει ένα δίκτυο ή να εισαγάγει υπερβολικό φορτίο κυκλοφορίας στο δίκτυο προκαλώντας αναμεταδόσεις και άρα ανεπαρκή δρομολόγηση. Το δεύτερο είδος απειλής προέρχεται από τους συμβιβασμένους κόμβους, οι οποίοι διαδίδουν ανακριβείς πληροφορίες δρομολόγησης σε άλλους κόμβους. Η ανίχνευση τέτοιων ανακριβών πληροφοριών είναι πολύ δύσκολη υπόθεση.

Για την προστασία από το πρώτο είδος απειλής, οι κόμβοι μπορούν να προστατεύσουν τις πληροφορίες δρομολόγησης με τον ίδιο τρόπο όπως προστατεύουν την μεταφορά δεδομένων, δηλαδή μέσω της χρήσης των κρυπτογραφικών σχεδίων όπως η ψηφιακή υπογραφή. Αυτό όμων δεν είναι αποτελεσματικό ενάντια στις επιθέσεις από τους συμβιβασμένους servers. Χειρότερα ακόμα, όπως έχουμε υποστηρίξει, δεν μπορούμε να παραμελήσουμε την δυνατότητα των κόμβων να συμβιβάζονται σε ένα ad-hoc

δίκτυο. Η ανίχνευση των συμβιβασμένων κόμβων μέσω της δρομολόγησης των πληροφοριών είναι επίσης δύσκολη σε ένα ad-hoc δίκτυο λόγω της δυναμικά μεταβαλλόμενης τοπολογίας της. Όταν ένα μέρος της πληροφορίας βρεθεί άκυρο, οι πληροφορίες θα μπορούσαν να παραχθούν από έναν συμβιβασμένο κόμβο, ή θα μπορούσε να θεωρηθεί άκυρο το αποτέλεσμα των αλλαγών τοπολογίας.

Αφ' ετέρου, μπορούμε να εκμεταλλευτούμε ορισμένες ιδιότητες των ad-hoc δικτύων για να επιτύχουμε ασφαλή δρομολόγηση. Τα πρωτόκολλα δρομολόγησης στα ad-hoc δίκτυα πρέπει να χειριστούν την ξεπερασμένη πληροφορία δρομολόγησης για να προσαρμόσουν τη δυναμικά μεταβαλλόμενη τοπολογία. Οι λανθασμένες πληροφορίες δρομολόγησης που παρήχθησαν από τους συμβιβασμένους κόμβους θα μπορούσαν, ως ένα ορισμένο βαθμό, να θεωρηθούν ξεπερασμένες πληροφορίες. Εφ' όσον υπάρχουν αρκετοί σωστοί κόμβοι, το πρωτόκολλο δρομολόγησης πρέπει να είναι σε θέση να βρεί τις διαδρομές που πηγαίνουν γύρω από αυτούς τους συμβιβασμένους κόμβους. Αυτή η ικανότητα των πρωτοκόλλων δρομολόγησης στηρίζεται συνήθως στις πλεονάζουσες πολλαπλές διαδρομές μεταξύ των κόμβων στα ad-hoc δίκτυα. Εάν τα πρωτόκολλα δρομολόγησης ανακαλύψουν πολλαπλές διαδρομές (π.χ.,τα πρωτόκολλα ZRP, DSR, TORA, και AODV μπορούν να το επιτύχουν αυτό), οι σταθμοί μπορούν να εταπηδήσουν σε μια εναλλακτική διαδρομή όταν εμφανίζεται πρόβλημα στην αρχική διαδρομή.

Η diversity κωδικοποίηση εκμεταλλεύεται τις πολλαπλές διαδρομές με έναν αποδοτικό τρόπο χωρίς αναμετάδοση μηνυμάτων. Η βασική ιδέα είναι να διαβιβαστούν οι περιττές πληροφορίες μέσω των πρόσθετων διαδρομών για την ανίχνευση και τη διόρθωση λάθους. Παραδείγματος χάριν, εάν υπάρχουν χ διαδρομές μεταξύ δύο σταθμών, μπορούμε να χρησιμοποιήσουμε το χ - ρ κανάλια για να διαβιβάσουμε τα δεδομένα και να χρησιμοποιήσουμε τα άλλα ρ κανάλια για να διαβιβάσουμε τις πλεονάζουσες πληροφορίες. Ακόμα κι αν ορισμένες διαδρομές εκτεθούν, ο δέκτης μπορεί ακόμα να είναι σε θέση να επικυρώσει τα μηνύματα και να τα ανακτήσει από τα λάθη χρησιμοποιώντας τις πλεονάζουσες πληροφορίες από τα πρόσθετα ρ κανάλια.[5]

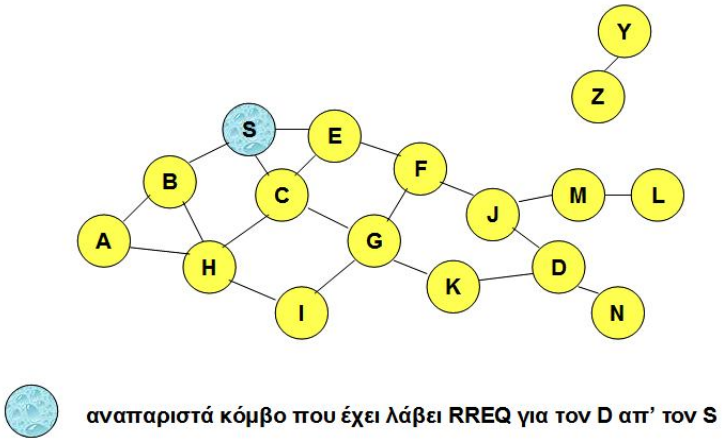
7.1 DSR (DYNAMIC SOURCE ROUTING)

Το DSR είναι reactive πρωτόκολλο που βασίζεται στην προσέγγιση δρομολόγησης πηγής (source route). Η βασική αρχή αυτής της προσέγγισης είναι ότι επιλέγεται όλη η διαδρομή από την πηγή και τοποθετείται σε κάθε πακέτο που στέλνεται. Κάθε κόμβος κρατά στη μνήμη του τις δρομολογήσεις πηγής που έμαθε.

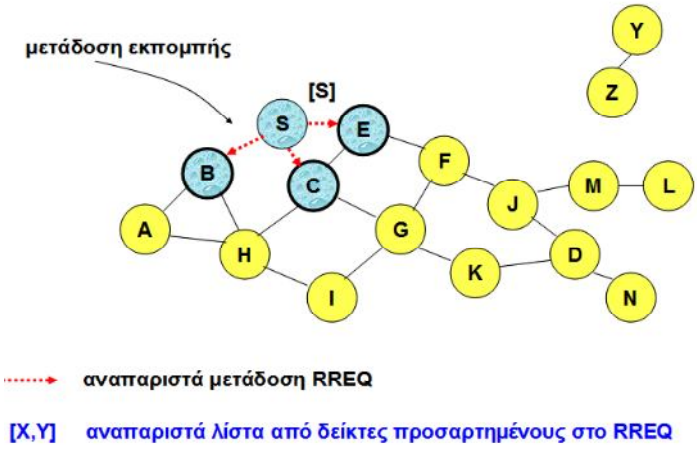
Όταν πρέπει να στείλει ένα πακέτο, πρώτα ελέγχει μέσα στη μνήμη του για την ύπαρξη τέτοιας διαδρομής. Αν δεν είναι διαθέσιμος μέσα στη μνήμη ο κατάλληλος προορισμός, ο κόμβος πραγματοποιεί μία εύρεση διαδρομής εκπέμποντας πακέτο ερώτησης (RREQ) μέσω του δικτύου. Όταν λάβει το RREQ, ο κόμβος ψάχνει μια διαδρομή μέσα στη μνήμη του για τον προορισμό του RREQ. Όταν τη βρει, στέλνει πακέτο απάντησης (RREP) στην πηγή. Εν τούτοις, αν δεν υπάρχει κατάλληλη διαδρομή ο κόμβος προσθέτει τη διεύθυνσή του στο RREQ και συνεχίζει να εκπέμπει.

Όταν ένας κόμβος ανιχνεύσει μια αποτυχία διαδρομής, στέλνει πακέτο λάθους (RER) στην πηγή που χρησιμοποιεί την ίδια ζεύξη και μετά ξαναρχίζει τη διαδικασία εύρεσης διαδρομής.[14]

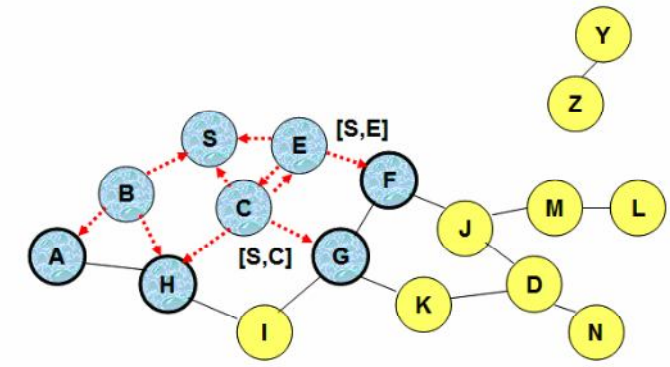
Η ανακάλυψη δρομολογίου φαίνεται στις Εικόνες 27, 28, 29, 30, 31 και 32:



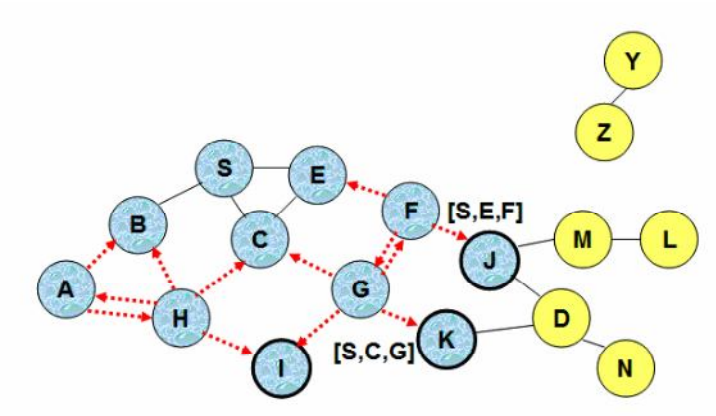
Εικόνα 27. Ο κόμβος αφετηρία S 'πλημμυρίζει' ένα πακέτο Αίτησης Δρομολογίου (Route Request - RREQ)



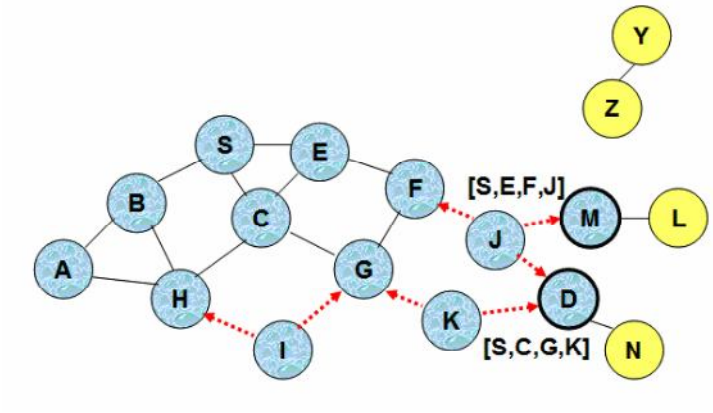
Εικόνα 28. Αρχίζει η μετάδοση εκπομπής του RREQ



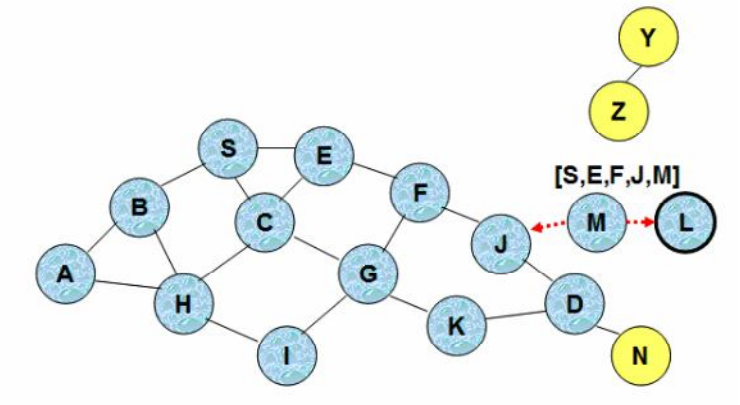
Εικόνα 29. Ο κόμβος Η δέχεται πακέτο από δύο γείτονες: πιθανότητα σύγκρουσης



Εικόνα 30. Ο κόμβος C δέχεται RREQ από τον G και τον H αλλά δεν το προωθεί ξανά γιατί ο κόμβος C έχει
ήδη προωθήσει RREQ μια φορά

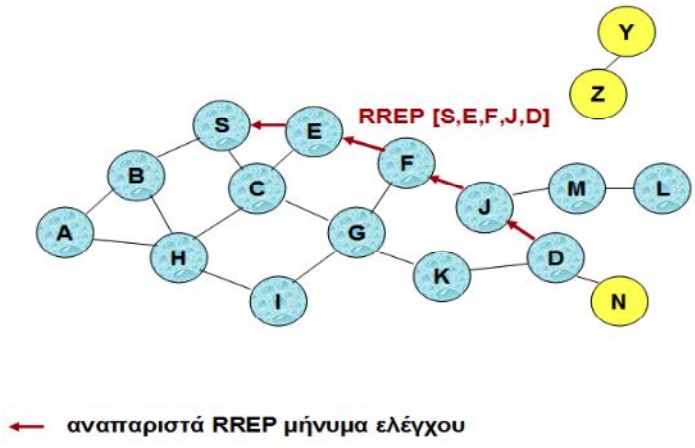


Εικόνα 31. Οι κόμβοι J και K μεταδίδουν και οι δύο RREQ στον κόμβο D. Εφόσον οι κόμβοι J και K κρύβονται ο ένας από τον άλλο, οι μεταδόσεις τους μπορεί να συγκρουστούν



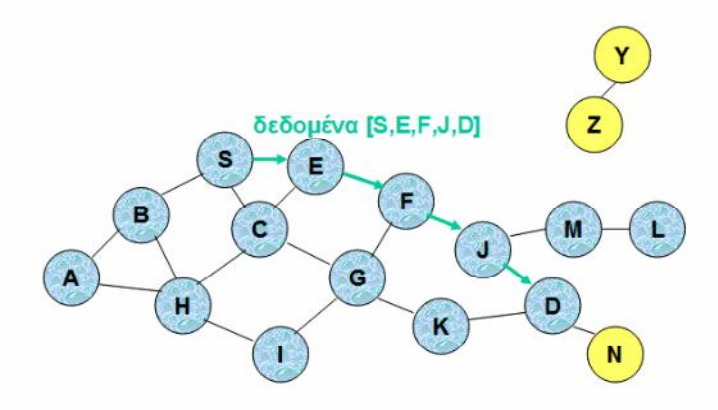
Εικόνα 32. Ο κόμβος D δεν προωθεί RREQ, γιατί είναι ο επιθυμητός στόχος της ανακάλυψης του δικτύου

Η απάντηση δρομολογίου φαίνεται στην Εικόνα 33:



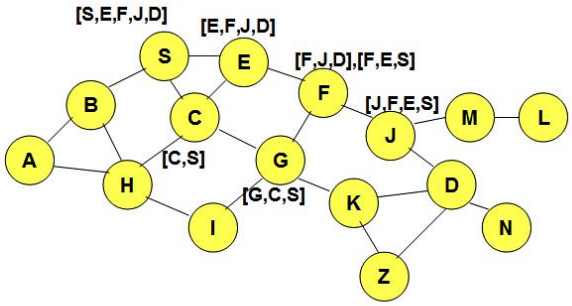
Εικόνα 33. Ο προορισμός D λαμβάνοντας το πρώτο RREQ, στέλνει ένα πακέτο Απάντησης Δρομολογίου (Route Reply - RREP) μέσω του αντίστροφου δρομολογίου. Το RREP περιλαμβάνει το δρομολόγιο από τον S στον D, μέσω του οποίου το RREQ έφτασε στον κόμβο D

Η παράδοση δεδομένων στο DSR φαίνεται στην ακόλουθη Εικόνα (Εικόνα 34):



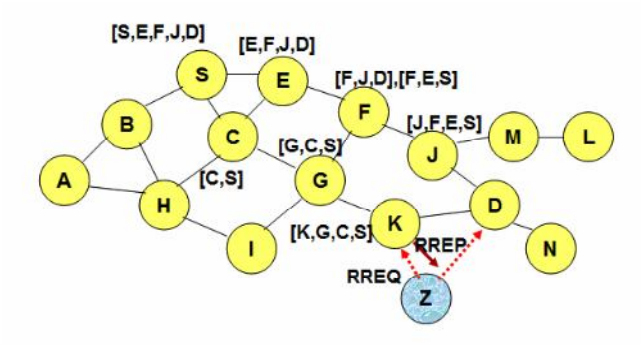
Εικόνα 34. Ο κόμβος S δεχόμενος το RREP, αποθηκεύει το δρομολόγιο που περιέχεται στο RREP. Όταν ο κόμβος S στέλνει ένα πακέτο δεδομένων στον D, ολόκληρο το δρομολόγιο περιέχεται στην επικεφαλίδα του πακέτου γι' αυτό και το όνομα δρομολόγηση πηγής. Οι ενδιάμεσοι κόμβοι χρησιμοποιούν το πηγαίο δρομολόγιο που περιέχεται σε ένα πακέτο, για να καθορίσουν σε ποιόν πρέπει να προωθηθεί το πακέτο

Στις Εικόνες 35, 36 και 37 που έπονται, παρουσιάζεται η χρήση της αποθήκευσης δρομολογίων:

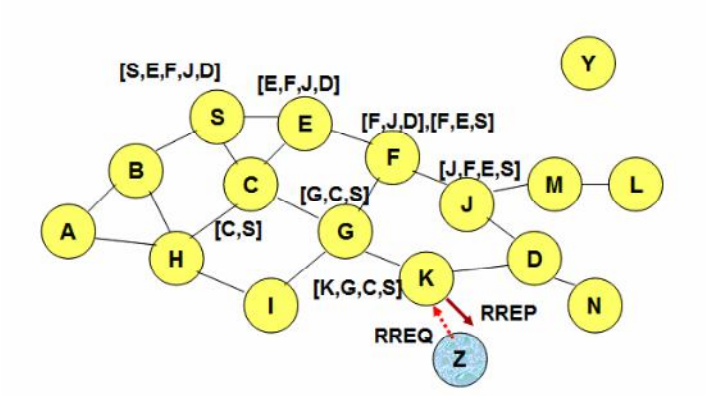


[P,Q,R] αναπαριστά αποθηκευμένο δρομολόγιο σε κόμβο
(το DSR διατηρεί τα αποθηκευμένα δρομολόγια σε δενδροειδή διάταξη)

Εικόνα 35. Όταν ο κόμβος S μαθαίνει πως ένα δρομολόγιο προς τον κόμβο D καταστρέφεται, χρησιμοποιεί ένα άλλο δρομολόγιο απ' την τοπική του μνήμη, αρκεί ένα τέτοιο δρομολόγιο προς τον D να υπάρχει εκεί -αλλιώς, ο κόμβος S αρχικοποιεί νέα ανακάλυψη μονοπατιού

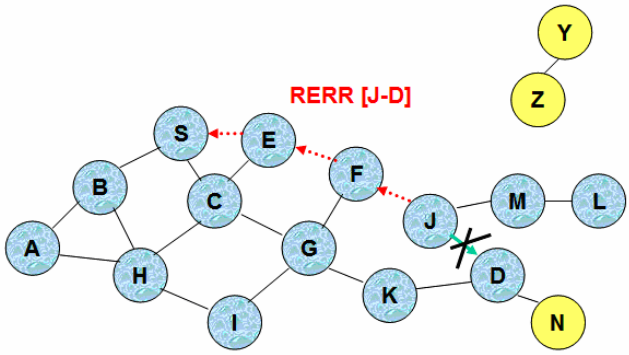


Εικόνα 36. Όταν ο κόμβος Z στέλνει μια αίτηση δρομολογίου για τον κόμβο C, ο κόμβος K επιστρέφει μια απάντηση δρομολογίου [Z,K,G,C] προς τον κόμβο Z, συνήθως χρησιμοποιώντας αποθηκευμένο δρομολόγιο



Εικόνα 36. Έστω ότι δεν υπάρχει σύνδεσμος ανάμεσα στον D και τον Z. Η Απάντηση Δρομολογίου (RREP) απ' τον K περιορίζει το 'πλημμύρισμα' των RREQ

Τέλος, παρουσιάζεται σχηματικά (Εικόνα 37) το σφάλμα δρομολογίου (RER):

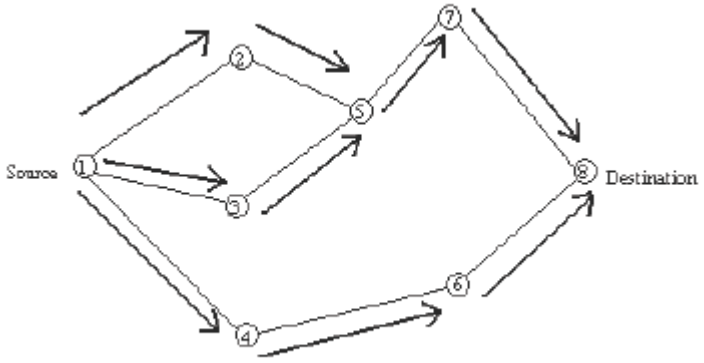


Εικόνα 37. Ο J στέλνει ένα Σφάλμα Δρομολογίου στον S κατά μήκος του δρομολογίου J-F-E-S, όταν η προσπάθειά του να προωθήσει ένα πακέτο δεδομένων του S (με δρομολόγιο SEFJD) μέσω του J-D αποτυγχάνει οι κόμβοι που 'ακούν' το RERR ανανεώνουν τα αποθηκευμένα δρομολόγιά τους, για να αφαιρέσουν το σύνδεσμο J-D

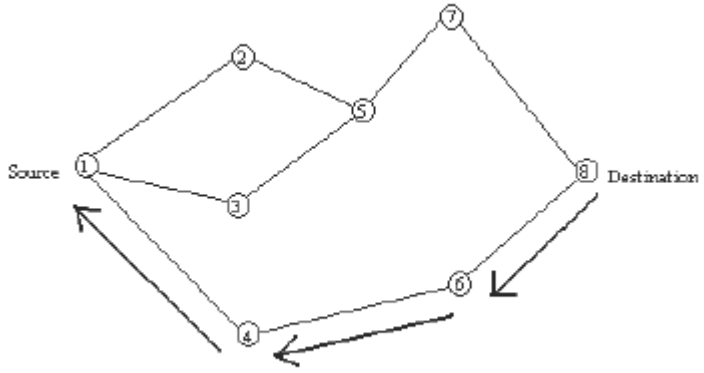
7.2 AODV (AD HOC ON-DEMAND DISTANCE VECTOR)

Το AODV είναι πρωτόκολλο δρομολόγησης hop-by-hop. Όταν ένας κόμβος πρέπει να στείλει ένα πακέτο δεδομένων σε έναν προορισμό στον οποίο δεν έχει διαδρομή, πρέπει να εκπέμψει ένα RREQ σε όλους του τους γείτονες. Κάθε γείτονας το κάνει αυτό μέχρι να φτάσει στον προορισμό του (ή ένας κόμβος με έγκυρη διαδρομή στον προορισμό). Αυτός ο κόμβος στέλνει ένα RREP πακέτο που ταξιδεύει το αντίστροφο μονοπάτι μέχρι να φτάσει την πηγή. Πάνω από τη λήψη της απάντησης κάθε μεσάζον αναβαθμίζει το δικό του routing table. Με αυτόν τον τρόπο «χτίζεται» μία διαδρομή ανάμεσα στην πηγή και στον προορισμό. Διαφορετικά από το DSR, η πηγή δε χρησιμοποιεί όλη τη διαδρομή μέσα στα εξερχόμενα πακέτα.

Μάλλον, η απόφαση για το επόμενο hop παίρνεται ξεχωριστά μετά από κάθε hop. Εφόσον στηρίζεται στην αρχή του παράγοντα απόστασης (distance vector principle), οι AODV αναθέσεις αυξάνουν μονότονα τις ακολουθίες αριθμών στις διαδρομές, οι οποίες καθορίζουν την ανανέωση των διαδρομών, όπως και τη μέτρηση των hop (hop count) η οποία καθορίζει τη βέλτιστη διαδρομή.[15]



(a) Propogation of Route Request (RREQ) Packet



(b) Path taken by the Route Reply (RREP) Packet

Εικόνα 38. Λειτουργία του AODV

7.2.1 Ανεπιφύλακτη Έμπιστη Σχέση Μεταξύ Γειτόνων

Τα τρέχοντα ad-hoc πρωτόκολλα δρομολόγησης έμφυτα εμπιστεύονται όλους τους συμμετέχοντες. Τα περισσότερα ad-hoc πρωτόκολλα δρομολόγησης είναι συνεργάσιμα από φύση τους και εξαρτώνται από τους γειτονικούς κόμβους μέχρι τα πακέτα διαδρομής. Αυτό το αφελές μοντέλο εμπιστοσύνης επιτρέπει στους κακόβουλους κόμβους να παραλύουν ένα ad-hoc δίκτυο με την εισαγωγή εσφαλμένων αναβαθμίσεων δρομολόγησης, την επανάληψη παλιών μηνυμάτων, την αλλαγή των αναβαθμίσεων δρομολόγησης ή τη διαφήμιση λανθασμένων πληροφοριών δρομολόγησης. Καθώς αυτές οι επιθέσεις είναι πιθανές και σε δίκτυο με υποδομή (fixed network), το ad-hoc περιβάλλον τις μεγεθύνει και κάνει δύσκολη την ανίχνευσή τους.

7.2.2 Απόδοση (Throughput)

Τα ad-hoc δίκτυα μεγιστοποιούν την ολική απόδοση (throughput) του δικτύου χρησιμοποιώντας όλους τους διαθέσιμους κόμβους για δρομολόγηση και προώθηση.

Εν τούτοις, ένας κόμβος μπορεί να έχει κακή συμπεριφορά με το να συμφωνεί στην προώθηση πακέτων και μετά αποτυγχάνει στο να το κάνει, επειδή είναι υπερφορτωμένος (overloaded), εγωιστής (selfish), κακόβουλος (malicious) ή καταστραμμένος (broken). Οι κόμβοι με κακή συμπεριφορά μπορεί να αποτελέσουν σημαντικό πρόβλημα. Αν και η μέση απώλεια στην απόδοση οφείλεται στην κακή συμπεριφορά των κόμβων και δεν είναι τόσο υψηλή, στη χειρότερη περίπτωση είναι πολύ υψηλή.

7.2.3 Διαχείρηση κλειδιού (Key Management)

Η ασφάλεια στη δικτύωση εξαρτάται σε πολλές περιπτώσεις από κατάλληλη διαχείριση κλειδιού. Η διαχείριση κλειδιού αποτελείται από ποικίλες υπηρεσίες εκ των οποίων η καθεμία είναι ζωτικής σημασίας για την ασφάλεια των συστημάτων δικτύωσης. Οι υπηρεσίες πρέπει να εξασφαλίζουν λύσεις για να είναι σε θέση να απαντούν στις ακόλουθες ερωτήσεις:

Μοντέλο εμπιστοσύνης *(Trust model)*: πρέπει να έχουν καθοριστεί πόσα διαφορετικά στοιχεία στο δίκτυο μπορούν να εμπιστευτούν το ένα το άλλο. Το περιβάλλον και η περιοχή εφαρμογής του δικτύου επηρεάζουν ευρέως το απαιτούμενο μοντέλο εμπιστοσύνης. Συνεπώς, οι σχέσεις εμπιστοσύνης ανάμεσα στα στοιχεία του δικτύου, επηρεάζει τον τρόπο που το σύστημα διαχείρισης κλειδιού είναι κατασκευασμένο στο δίκτυο.

Κρυπτοσυστήματα *(Cryptosystems)*: διαθέσιμα για τη διαχείριση του κλειδιού. Σε κάποιες περιπτώσεις μόνο οι δημόσιοι ή οι συμμετρικοί μηχανισμοί κλειδιού μπορούν να εφαρμοστούν, καθώς σε άλλα γενικά πλαίσια είναι διαθέσιμα κρυπτοσυστήματα ελλειπτικής καμπύλης (*Elliptic Curve Cryptosystems* (*ECC*)). Ενώ η κρυπτογράφηση δημόσιου κλειδιού προσφέρει περισσότερη σιγουριά (π.χ. γνωστές ψηφιακές υπογραφές-digital signature schemes),τα κρυπτοσυστήματα των δημόσιων κλειδιών είναι σημαντικά πιο αργά από τα αντίγραφα των μυστικών κλειδιών τους, όταν χρειάζεται παρόμοιο επίπεδο ασφαλείας. Αντιθέτως, τα συστήματα μυστικών κλειδιών προσφέρουν λιγότερη λειτουργικότητα και υποφέρουν πιο πολύ από προβλήματα, π.χ. διανομή κλειδιού (key distribution). Τα ECC κρυπτοσυστήματα είναι νεότερο πεδίο κρυπτογράφησης αλλά ήδη χρησιμοποιούνται ευρέως όπως για παράδειγμα στα συστήματα έξυπνων καρτών (smart card systems).

Δημιουργία κλειδιού *(Key creation)*: πρέπει να καθοριστεί ποιες ομάδες χρηστών (parties) επιτρέπεται να παράγουν κλειδιά για τους εαυτούς τους ή για άλλες ομάδες και τι είδος κλειδιού.

Αποθήκευση κλειδιού *(Key storage):* στα ad-hoc δίκτυα μπορεί να μην υπάρχει κεντραρισμένη αποθήκευση για τα κλειδιά. Ούτε να υπάρχει αποθηκευμένο αντίγραφο διαθέσιμο για ελάχιστη ανοχή (fault tolerance). Στα ad-hoc δίκτυα οποιοδήποτε στοιχείο δικτύου ενδεχομένως να πρέπει να αποθηκεύσει το κλειδί του όπως επίσης και πιθανά κλειδιά άλλων στοιχείων. Επιπλέον τα κοινά μυστικά (shared secrets) εφαρμόζονται προκειμένου να διανέμουν τα τμήματα του κλειδιού σε διάφορους κόμβους. Σε τέτοιου είδους συστήματα η συμμόρφωση (compromising) ενός κόμβου δεν προβαίνει ακόμα σε συμβιβασμό με τα μυστικά κλειδιά.

Διανομή κλειδιού *(Key distribution)*: η υπηρεσία διαχείρισης κλειδιού πρέπει να σιγουρευτεί ότι τα παραγόμενα κλειδιά διανέμονται με ασφαλή τρόπο στους ιδιοκτήτες τους. Όποιο κλειδί πρέπει να κρατηθεί μυστικό, πρέπει να διανεμηθεί έτσι ώστε η εμπιστευτικότητα, η αυθεντικοποίηση και η ακεραιότητα δεν έχουν παραβιαστεί. Για παράδειγμα όταν εφαρμόζονται συμμετρικά κλειδιά και οι δύο ή όλη η παρέα (parties) που εμπλέκονται, πρέπει να παραλάβουν το κλειδί με ασφαλή

τρόπο. Στην κρυπτογράφηση δημόσιου κλειδιού, ο μηχανισμός διανομής κλειδιού πρέπει να εγγυηθεί ότι τα ιδιωτικά κλειδιά παραδίδονται μόνο στους εξουσιοδοτημένους χρήστες. Η διανομή των δημόσιων κλειδιών δε χρειάζεται να προστατέψει την εμπιστευτικότητα, αλλά η ακεραιότητα και η αυθεντικοποίηση των κλειδιών πρέπει να έχουν εξασφαλιστεί.[4]

ΚΕΦΑΛΑΙΟ 8^{Ο}

8. Ασφάλεια πρωτοκόλλου MAC

8.1 Απρεπής συμπεριφορά στα κανάλια πρόσβασης

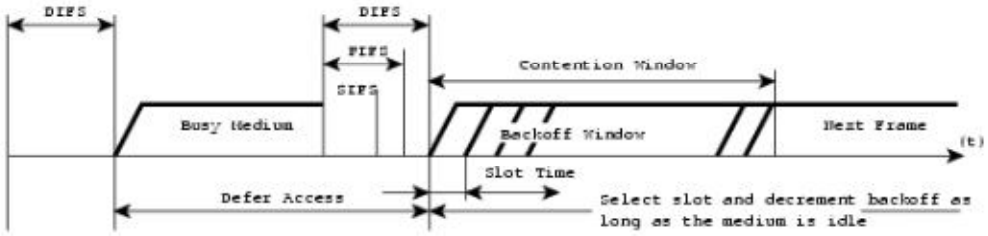
Το πρόβλημα

Δεδομένου ότι δεν υπάρχει καμία κεντρική αρχή στα Ad-Hoc, ασύρματα πρωτόκολλα ενδιάμεσου ελέγχου πρόσβασης (MAC), όπως το IEEE 802.11, χρησιμοποιούν μηχανισμούς contention resolution για το διαμοιρασμό του ασύρματου καναλιού. Το contention resolution είναι τυπικά βασισμένο σε συνεταιριστικούς μηχανισμούς που εξασφαλίζουν ένα λογικό μερίδιο του καναλιού για όλους τους συμμετέχοντες κόμβους. Σε αυτό το περιβάλλον, μερικοί εγωιστικοί hosts στο δίκτυο μπορούν να συμπεριφερθούν απρεπώς με το να αποτυγχάνουν να εμμείνουν στο πρωτόκολλο MAC, με την πρόθεση της λήψης ενός άδικου μεριδίου του καναλιού. Η παρουσία εγωιστικών κόμβων που παρεκκλίνουν από το πρωτόκολλο contention resolution μπορεί να μειώσει το μερίδιο απόδοσης που παραλαμβάνεται από τους προσαρμοσμένους κόμβους.

Το IEEE 802.11 πρωτόκολλο MAC, που είναι το τυποποιημένο πρωτόκολλο MAC για τα ασύρματα δίκτυα, έχει δύο μηχανισμούς για το contention resolution: ένας κεντραρισμένος μηχανισμός που καλείται PCF (Point Coordination Function: λειτουργία συντονισμού σημείου) και ένας πλήρως διανεμημένος μηχανισμός που καλείται DCF (Distributed Coordination Function: διανεμημένη λειτουργία συντονισμού). Η PCF χρειάζεται έναν κεντραρισμένο ελεγκτή (όπως ένα σταθμό βάσεων) και μπορεί μόνο να χρησιμοποιηθεί στα βασισμένα σε υποδομή δίκτυα, κατά συνέπεια δεν πρόκειται να ληφθεί υπόψη στον ad-hoc τρόπο. Αντίθετα, η DCF χρησιμοποιείται ευρέως στα βασισμένα σε υποδομή ασύρματα δίκτυα καθώς επίσης και στα ad hoc ασύρματα δίκτυα.

Η DCF χρησιμοποιείται από το δίκτυο 802.11 κι αποτελείται από δύο βασικά συστατικά: 1) Interframe space (IFS) και 2) random backoff (παράθυρο ανταγωνισμού-contention window). Το IFS επιτρέπει στο 802.11 να ελέγχει ποια κίνηση (traffic) έχει πρώτη πρόσβαση στο κανάλι εφόσον ο φορέας Carrier Sense δηλώνει ότι το κανάλι είναι ελεύθερο.

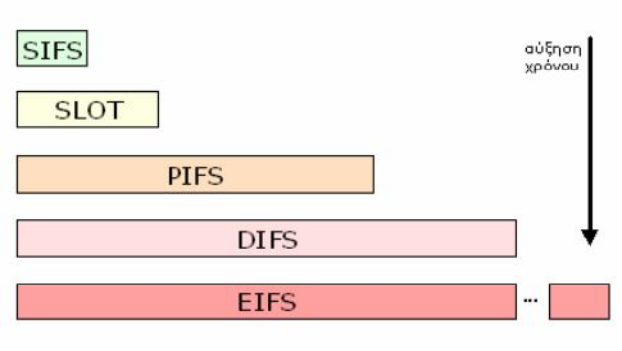
1) Interframe space (IFS)



Εικόνα 39. Interframe Spaces (IFSs)

Το πρότυπο 802.11 ορίζει τα ακόλουθα interframe spaces:

- Short Interframe Space (SIFS). Το μικρότερο χρονικά διάστημα. Χρησιμοποιείται μεταξύ μεταδόσεων πλαισίων μεγίστης προτεραιότητας, αλληλουχίας κατατετμημένων πλαισίων, RTS/CTS, ACK.
- Slot: Βασική μονάδα χρόνου στο 802.11 MAC.
- Point (coordination function) Interframe Space (PIFS): SIFS + 1 Slot. Χρησιμοποιείται στην μέθοδο προσπέλασης PCF.
- Distributed (coordination function) interframe space (DIFS): SIFS + 2 Slot. Το μεγαλύτερο σταθερού μεγέθους διάστημα. Χρησιμοποιείται από όλους τους σταθμούς.
- EIFS: Μεταβλητό μέγεθος.



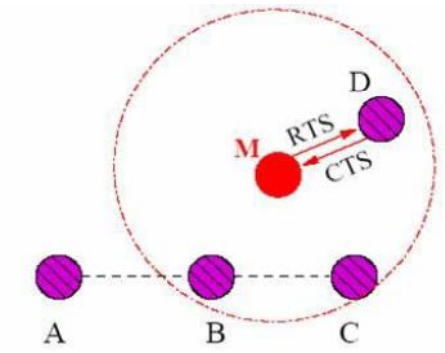
Εικόνα 40. Τα interframe spaces του προτύπου 802.11

2) Τυχαία Οπισθοχώρηση (Random Backoff)

Η DCF χρησιμοποιεί την επιλογή CSMA/CA (πολλαπλή πρόσβαση με ακρόαση φέροντος / αποφυγή σύγκρουσης Carrier Sense Multiple Access/Collision Avoidance) για το resolving contention μεταξύ των πολλαπλών κόμβων που έχουν πρόσβαση στο κανάλι. Ένας κόμβος (αποστολέας) με τα δεδομένα που διαβιβάζει στο κανάλι επιλέγει μια τυχαία backoff τιμή από τη σειρά [0;CW], όπου το CW (contention window-παράθυρο ανταγωνισμού) είναι μια μεταβλητή που διατηρείται από κάθε κόμβο. Ενώ το κανάλι είναι αδρανές, ο μετρητής backoff μειώνεται κατά ένα μετά από κάθε χρονοσχισμή (time slot) (ένα σταθερό διάστημα-interval του χρόνου) και ο μετρητής

παγώνει όταν το κανάλι απασχολείται. Ο κόμβος μπορεί να έχει πρόσβαση στο κανάλι όταν ο μετρητής backoff μειώνεται στο μηδέν.

Αφότου ο μετρητής backoff είναι στο μηδέν, ο αποστολέας μπορεί να διατηρήσει το κανάλι για τη διάρκεια της μεταφοράς δεδομένων με το να ανταλλάσσει πακέτα ελέγχου στο κανάλι. Ο αποστολέας αρχικά στέλνει ένα πακέτο RTS (αίτημα προς αποστολή) στο δέκτη, κατόπιν ο δέκτης αποκρίνεται με ένα CTS πακέτο (καθαρίστε για να στείλετε). Αυτή η ανταλλαγή RTS-CTS είναι προαιρετική στο IEEE 802.11. Στοχεύει στην εξασφάλιση της κράτησης (reservation) καναλιών κατά τη διάρκεια της μετάδοσης δεδομένων. Και τα δύο πακέτα περιέχουν την προτεινόμενη διάρκεια της μετάδοσης δεδομένων. Άλλοι κόμβοι που κρυφακούνε είτε το RTS είτε το CTS (ή και τα δύο) απαιτούνται για να αναβάλουν τις μεταδόσεις στο κανάλι κατά τη διάρκεια που διευκρινίζεται στο RTS/CTS.



Εικόνα 41. Οι κόμβοι M και D συνεννοούνται και παρεμβάλλονται στην επικοινωνία του μονοπατιού των κόμβων B και C

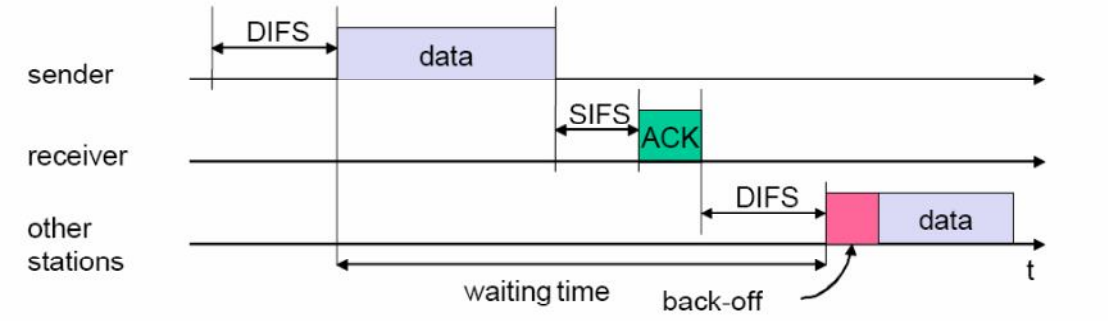
Μετά από μια επιτυχή ανταλλαγή RTS/CTS, ο αποστολέας διαβιβάζει ένα πακέτο δεδομένων, το οποίο θα αναγνωριστεί από ένα ACK. Εάν η μετάδοση δεδομένων του κόμβου είναι επιτυχής, ο κόμβος μηδενίζει το CW του σε μια ελάχιστη αξία (CWmin), διαφορετικά εάν ο αποστολέας δεν λαμβάνει το CTS, τότε το CW διπλασιάζεται, αλλά δεν πρέπει να υπερβεί μια μέγιστη αξία CWmax. Ένας κόμβος απρεπούς συμπεριφοράς μπορεί να λάβει περισσότερο από το σημαντικό μέρος του εύρους ζώνης:

- Επιλέγοντας backoff τιμές από μια διαφορετική διανομή με τη μικρότερη μέση backoff τιμή από τη διανομή που διευκρινίζεται από το DCF (π.χ., με την επιλογή backoff των τιμών από τη σειρά [0, CW/4] αντί της σειράς [0,CW]).
- Χρησιμοποιώντας μια διαφορετική στρατηγική αναμετάδοσης που δεν διπλασιάζει την τιμή CW μετά από τις συγκρούσεις. Σημειώνουμε ότι δεν είναι ευεργετικό για έναν εγωιστικό κόμβο να μην καθυστερηθεί καθόλου ή να επιλέξει μια πολύ μικρή σταθερή περίοδο, δεδομένου ότι αυτό μπορεί να οδηγήσει σε ένα πολύ υψηλό ποσοστό σύγκρουσης και στην απώλεια των πακέτων που στέλνει.

Τέτοια εγωιστική συμπεριφορά μπορεί σοβαρά να υποβιβάσει την απόδοση των καλά-συμπεριφερόμενων κόμβων. Για παράδειγμα, τα αποτελέσματα προσομοίωσης που επιτυγχάνονται από τους Kyasanur και Vaidya δείχνουν ότι σε ένα δίκτυο που περιέχει οκτώ κόμβους που στέλνουν πακέτα σε έναν κοινό δέκτη με έναν από τους οκτώ κόμβους να συμπεριφέρεται απρεπώς με το να επιλέγει backoff τιμές από τη σειρά [0,CW/4], η απόδοση των άλλων επτά κόμβων υποβιβάζεται κατά τουλάχιστον 50 τοις εκατό. Μέχρι στιγμής δεν υπάρχει καμία δημοσιευμένη λύση που προτείνεται σε αυτό το σύνθετο πρόβλημα, εκτός από τη λύση που προτείνεται από τους Kyasanur και Vaidya.

Συνοψίζουμε τη λειτουργία του DCF:

- Όταν μεταδίδεται ένα πακέτο, επιλέγεται ένα διάστημα οπισθοχώρησης μέσα στο εύρος τιμών [0, CW].
- Αντίστροφη μέτρηση όσο το κανάλι είναι αδρανές.
- Η αντίστροφη μέτρηση αναστέλλεται για τα διαστήματα που το κανάλι είναι ενεργό.
- Όταν φτάσει στο 0, μεταδίδεται RTS.
- Η επιλογή ενός μεγάλου CW οδηγεί σε μεγάλα διαστήματα οπισθοχώρησης, με αποτέλεσμα μεγαλύτερο overhead.
- Η επιλογή ενός μικρού CW οδηγεί σε μεγαλύτερο αριθμό συγκρούσεων (όταν δύο κόμβοι φτάσουν στο 0 συγχρόνως).
- Αφού ο αριθμός των κόμβων που προσπαθούν να μεταδώσουν την ίδια στιγμή μπορεί να αλλάζει με το χρόνο, απαιτείται κάποιος μηχανισμός για τη διαχείριση του ανταγωνισμού.
- IEEE 802.11 DCF: το παράθυρο ανταγωνισμού CW επιλέγεται δυναμικά, εξαρτώμενο από την συχνότητα εμφάνισης συγκρούσεων.
- Όταν ένας κόμβος δε λάβει CTS σε απάντηση κάποιου RTS που έστειλε, διπλασιάζει το cw (μέχρι κάποιο άνω όριο).
- Όταν ένας κόμβος ολοκληρώνει επιτυχημένα μια μεταφορά δεδομένων, επαναφέρει το CW σε CWmin.[10]



Εικόνα 42. Λειτουργία DCF

ΚΕΦΑΛΑΙΟ 9^{Ο}

9.Αυθεντικοποίηση

9.1 Εισαγωγή

Οι μηχανισμοί πιστοποίησης ταυτότητας προσπαθούν να επαληθεύσουν τη γνησιότητα των διαπιστευτηρίων (credentials) που δηλώνουν οι εμπλεκόμενοι. Κατά τις διαδικασίες αυθεντικοποίησης, μια συσκευή που επιθυμεί να γίνει μέρος ενός ασύρματου δικτύου θα πρέπει να αποδείξει στο δίκτυο ότι είναι *γνήσια.* Με τον όρο γνήσια εννοείται ότι αυτή δεν είναι πλαστή ή ότι δεν έχει υποστεί τροποποιήσεις τόσο στο λογισμικό όσο και στο υλικό της.

Τα περισσότερα αντικείμενα αξίας στον σημερινό κόσμο διαθέτουν κάποιο τρόπο για να αποδείξουν τη γνησιότητα τους. Χαρακτηριστικά, μπορούν να αναφερθούν τα χαρτονομίσματα. Αυτά διαθέτουν τη δυνατότητα να αποδείξουν ότι είναι γνήσια στο

σύνολο τους, αλλά συγχρόνως και ότι διαφέρουν μεταξύ τους βάσει ενός κωδικού αριθμού που διαθέτει το καθένα. Η αλλοίωση κάποιων στοιχείων ή χαρακτηριστικών τους (σκισίματα, φθορές, κλπ), δημιουργεί συνήθως υποψίες στον κάτοχό τους για τη γνησιότητα αυτών, οπότε καταφεύγει στις ανάλογες λύσεις.

Δυστυχώς, μέχρι στιγμής υπάρχουν πολύ λίγοι τρόποι μέσω των οποίων μπορεί να αποδειχθεί ότι ένα υπολογιστικό σύστημα είναι γνήσιο. Στην προσπάθεια να δοθεί απάντηση στη συγκεκριμένη ερώτηση, δηλαδή για το αν ένα υπολογιστικό σύστημα είναι γνήσιο μπορεί κάποιος να αποκριθεί ότι «δείχνει να είναι γνήσιο» και «συμπεριφέρεται με τον ενδεδειγμένο τρόπο» αλλά πάλι δεν είναι σε θέση να είναι σίγουρος. Πράγματι, στα υπολογιστικά συστήματα αυτή η απάντηση είναι και η σωστή αφού η δυναμική φύση του λογισμικού που διαθέτουν δεν επιτρέπει να προσδιορίσουμε εύκολα τυχόν τροποποιήσεις που έχουν υποστεί.

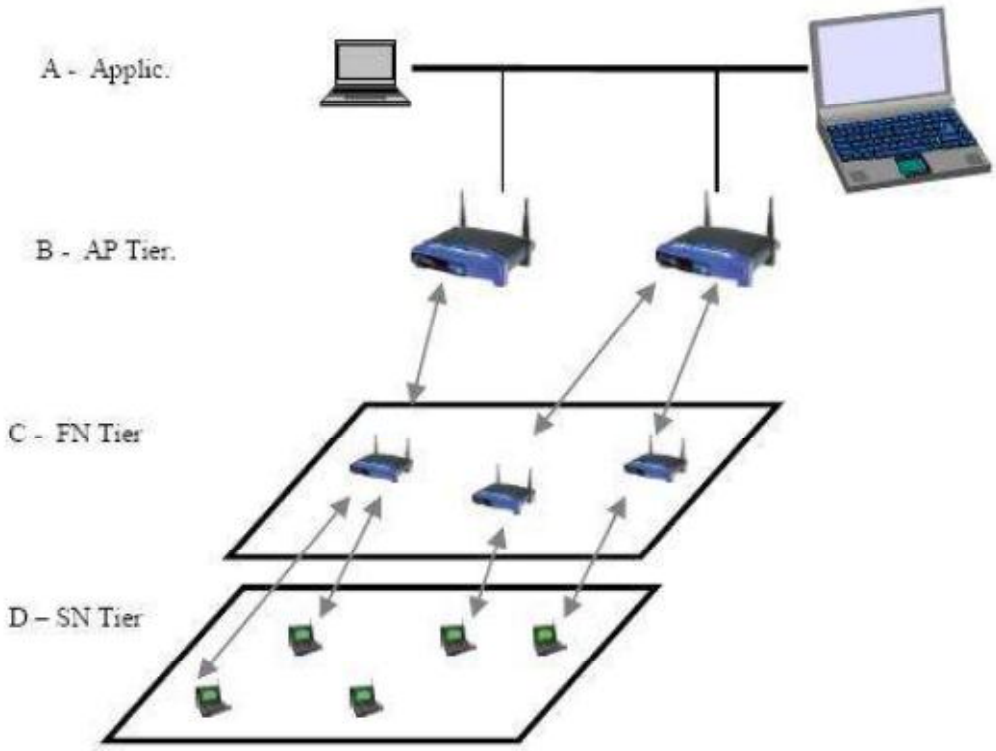
Προκειμένου να αποδειχθεί η γνησιότητα ενός υπολογιστικού συστήματος και η ικανότητα αυτού να αυθεντικοποιηθεί θα πρέπει να επαληθευθούν δύο πράγματα:

- Πρώτον, η συσκευή θα πρέπει να είναι ένα πραγματικό υπολογιστικό σύστημα με γνήσιες ιδιότητες και όχι ένας κακόβουλος χρήστης που μιμείται την συσκευή. Αν η συσκευή δεν είναι γνήσια, αλλά απομίμηση, το περιβάλλον διαχείρισης θα πρέπει να αποτρέψει την αυθεντικοποίηση.
- Δεύτερον, το υπολογιστικό σύστημα θα πρέπει να διαθέτει το ενδεδειγμένο λογισμικό (software) και σύστημα υλικού (hardware) ή και επιπλέον ιδιότητες που έχουν καθοριστεί και αναμένει ο διαχειριστής αυθεντικοποίησης. Αν όλα τα παραπάνω είναι πλήρως καθορισμένα τότε η συμπεριφορά του συστήματος είναι η αναμενόμενη. Κάθε πιθανή διαφοροποίηση δημιουργεί υπόνοιες και ενεργοποιεί μηχανισμούς άρνησης πρόσβασης

Παρακάτω αναλύονται οι υπάρχουσες προσεγγίσεις που έχουν γίνει στο χώρο των ασύρματων δικτύων για την αυθεντικοποίηση των συσκευών. Στο σύνολο τους είναι περιορισμένες και οι περισσότερες από αυτές καλύπτουν το θέμα επιφανειακά. Οι λύσεις που προτείνονται, απευθύνονται σε ορισμένα είδη δικτύων και δεν προτείνεται κάτι που να μπορεί να καλύψει όλο το εύρος των ασύρματων δικτύων.

9.2 Ad-Hoc Δίκτυα

Τα Ad-Hoc δίκτυα αποτελούν μια άλλη κατηγορία δικτύων με πολλές ιδιαιτερότητες. Η αυθεντικοποίηση στηρίζεται επί το πλείστον στην ιεράρχηση των ad-hoc δικτύων. Ιεραρχημένα ad-hoc δίκτυα θεωρούν αυτά που είναι χωρισμένα σε επίπεδα, με κάθε επίπεδο να περιλαμβάνει συσκευές που εκτελούν παρόμοιες εργασίες και έχουν ως σκοπό να υποστηρίξουν την λειτουργία των συσκευών των χρηστών. Η αυθεντικοποίηση στην προκειμένη περίπτωση στηρίζεται σε ένα μοντέλο όπου οι κόμβοι του δικτύου ζητάνε από τους γειτονικούς σε αυτούς κόμβους να δημιουργήσουν σχέσεις εμπιστοσύνης. Ακολούθως οι σχέσεις αυτές χρησιμοποιούνται ως βάση για να πραγματοποιηθεί η αυθεντικοποίηση.



Εικόνα 43.

Κάθε οντότητα διατηρεί μια λίστα με τις έμπιστες οντότητες. Χρησιμοποιεί, δε, αυτήν την λίστα κάθε φορά που επιθυμεί να δημιουργήσει ένα κανάλι επικοινωνίας μεταξύ δύο ή περισσοτέρων συσκευών. Η αυθεντικοποίηση των εισερχόμενων συσκευών στο δίκτυο στηρίζεται στην ανταλλαγή ενός μυστικού που ελέγχεται μέσω κάποιον εφαρμογών. Το μυστικό αυτό δεν είναι τίποτα άλλο από ένα σύνολο δεδομένων που αποτελεί το συνθηματικό των συσκευών, το οποίο υπολογίζεται μέσω των εφαρμογών λογισμικού.

Όπως συμβαίνει σε οποιαδήποτε διαδικασία αυθεντικοποίησης, κάθε εισερχόμενη συσκευή θα πρέπει να αποδείξει ότι έχει το δικαίωμα εισόδου. Τα δεδομένα δεν θεωρούνται έμπιστα μέχρι αποδείξεως του αντιθέτου. Για αυτό το λόγο κάθε συσκευή είναι εφοδιασμένη με ένα πιστοποιητικό (iCert) το οποίο και εκδίδεται από μια τρίτη έμπιστη οντότητα (TTP), η οποία αποτελεί μέλος του δικτύου. Η οντότητα αυτή δεν είναι τίποτα περισσότερο από μια συσκευή που είναι ικανή να δημιουργεί υπογραφές RSA, των οποίων το δημόσιο κλειδί είναι γνωστό σε όλες τις συσκευές που έχουν την δυνατότητα να επαληθεύσουν τις RSA υπογραφές.

Όταν το σημείο πρόσβασης Β ή μια συσκευή χρήστη Δ θέλει να γίνει μέλος του δικτύου, θα πρέπει να παρουσιάσει το πιστοποιητικό (iCert). Αυτό θα ελεγχθεί από μια εφαρμογή Α για την γνησιότητα του.

Αν το πιστοποιητικό (iCert) είναι το γνήσιο, η εφαρμογή Α θα ιδρύσει ένα κοινό μυστικό Κ Α, Β ή Κ Α, Δ , με το οποίο θα δίνεται η δυνατότητα στην συσκευή να επικοινωνήσει με την εφαρμογή. Σε περίπτωση που η συσκευή είναι μέλος του δικτύου το πιστοποιητικό (iCert) γίνεται λιγότερο σημαντικό. Για το διάστημα που οι συσκευές Β, Δ δεν διακόπτουν την σύνδεση, η σχέση εμπιστοσύνης που έχει δημιουργηθεί διατηρείται. Επιπλέον όμως κάθε συσκευή θα πρέπει να αυθεντικοποιηθεί και με τα υπόλοιπα μέλη του δικτύου αφού η τοπολογίες των adhoc δικτύων αλλάζουν συνεχώς,

με πολλές εξόδους και εισόδους διαφορετικών οντοτήτων. Η εφαρμογή Α δίνει την δυνατότητα αυτή εκδίδοντας περιοδικά νέα πιστοποιητικά για κάθε σημείο πρόσβασης ή απλής συσκευής.

Έχοντας ένα δίκτυο με πιστοποιημένες συσκευές που έχουν δημιουργήσει σχέσεις εμπιστοσύνης μπορούμε να δημιουργήσουμε μια υπηρεσία αυθεντικοποίησης δεδομένων. Η αυθεντικοποίηση αυτή θα διασφαλίσει τόσο την ακεραιότητα των δεδομένων αλλά συγχρόνως θα έχει ως αποτέλεσμα επιπλέον αποτελέσματα αυθεντικοποίησης αφού για την ανταλλαγή των δεδομένων θα χρησιμοποιηθούν και πάλι τα ήδη παραχθέντα πιστοποιητικά.

Τα πιστοποιητικά που εκδίδονται βασίζονται πάνω στο πρωτόκολλο TESLA, το οποίο και χρησιμοποιεί τεχνικές ασύμμετρης κρυπτογραφίας που είναι κατάλληλες για συσκευές που χρησιμοποιούν περιορισμένης διάρκειας πηγές ενέργειας. Τονίζεται ότι μόνο για το σημείο πρόσβασης απαιτούνται ισχυρές υπολογιστικές δυνατότητες μιας και αυτό θα δημιουργεί τα πιστοποιητικά και τις RSA υπογραφές.

Η αυθεντικοποίηση των συσκευών στην παραπάνω περιγραφή επιτυγχάνεται αφού τα πιστοποιητικά που δημιουργούνται αφορούν την συσκευή και όχι τον χρήστη. Αυτά αποθηκεύονται εντός της συσκευής και ο χρήστης δεν μπορεί να παρέμβει ούτε για να τα τροποποιήσει ούτε και να τα χρησιμοποιήσει σε άλλη συσκευή.

9.3. Άλλες Λύσεις

Πολλοί οργανισμοί προσπαθώντας να αυξήσουν τα επίπεδα ασφαλείας των ασύρματων δικτύων προτείνουν διάφορες λύσεις. Οι περισσότερες από αυτές στηρίζονται στην αυθεντικοποίηση των ασύρματων συσκευών, χρησιμοποιώντας φορητές μνήμες τύπου Flash ή έξυπνες κάρτες (smart cards). Στην συγκεκριμένη περίπτωση οι απόψεις διίστανται για το κατά πόσο η χρήση τέτοιων μεθόδων γίνεται προκειμένου να αυθεντικοποιηθεί ο χρήστης ή η συσκευή.

Οι έξυπνες κάρτες και οι φορητές μνήμες διαθέτουν πιστοποιητικά που έχουν εκδοθεί βάση της ταυτότητας του χρήστη. Η ενσωμάτωση όμως του εξοπλισμού που αναγνωρίζει τόσο τις κάρτες, όσο και τις φορητές μνήμες πάνω στις ασύρματες συσκευές διαφοροποιεί αυτήν την κατάσταση. Έτσι, πολλοί επικαλούνται ότι τα πιστοποιητικά μπορεί να εκδίδονται για τον χρήστη, αλλά χωρίς αυτά ούτε ο ίδιος, αλλά ούτε και η συσκευή μπορεί να αυθεντικοποιηθεί στον δίκτυο. Ουσιαστικά η προαναφερθείσα περιγραφή αποτελεί μια υβριδική μέθοδο αυθεντικοποίησης.

1. Έξυπνες Κάρτες

Η έξυπνη κάρτα διαθέτει όλες εκείνες τις πληροφορίες που χρειάζονται προκειμένου ο χρήστης να αυθεντικοποιηθεί στην ασύρματη συσκευή. Η τελευταία διαθέτει ενσωματωμένο υλικό (hardware) μέσω του οποίου τοποθετείται και γίνεται η ανάγνωση της κάρτας.

Το συγκεκριμένο υλικό συνοδεύεται και από κατάλληλο λογισμικό προκειμένου να γίνουν οι διαδικασίες αυθεντικοποίησης. Το σημαντικότερο είδος λογισμικού είναι η εκάστοτε εφαρμογή που κάνει την πιστοποίηση. Στην αρχή ο χρήστης θα δώσει τον μυστικό κωδικό προκειμένου να γίνει δεκτός από την συσκευή. Αμέσως μετά, ξεκινάει

ένας διάλογος μεταξύ της συσκευής και της κάρτας. Ο διάλογος αυτός έχει ως σκοπό να διαπιστώσει την αυθεντικότητα της κάρτας του χρήστη.

Μετά το πέρας αυτής τις διαδικασίας τα πιστοποιητικά που διαθέτει η κάρτα χρησιμοποιούνται προκειμένου να αναπαραχθεί ουσιαστικά ένας άλλος κωδικός, ο οποίος και θα χρησιμοποιηθεί όταν η συσκευή θελήσει να εισέλθει σε ένα δίκτυο. Το πρωτόκολλο που χρησιμοποιείται είναι το πρωτόκολλο πρόκλησης-απάντησης, ενώ οι ενέργειες που λαμβάνουν χώρα δεν διαφέρουν κατά πολύ αυτών του GSM.

Η παραπάνω φιλοσοφία, αποτελεί μια καλή λύση αυθεντικοποίησης, η οποία όμως είναι απαγορευτική για πολλούς, λόγω υψηλού κόστους. Επιπλέον, μπορεί να εφαρμοστεί μόνο σε ορισμένου τύπου δίκτυα .[10]

2. Flash Μνήμες

Πολλοί κατασκευαστές στηριζόμενοι στην φιλοσοφία λειτουργίας των έξυπνων καρτών προσπάθησαν να επινοήσουν πρακτικότερες μεθόδους. Μια από αυτές ήταν να χρησιμοποιήσουν φορητές μνήμες (flash memory). Σε αυτήν την περίπτωση το πιστοποιητικό χωρίζεται σε δύο ίσα μέρη. Το ένα μέρος αποθηκεύεται στην φορητή μνήμη και το άλλο στην ασύρματη συσκευή.

Επιπλέον αξίζει να αναφερθεί ότι πολλές φορές εκδίδονται επιπλέον τρία πιστοποιητικά, εκ των οποίων το ένα το γνωρίζει ο χρήστης, το άλλο η συσκευή και το τελευταίο είναι αποθηκευμένο στην φορητή μνήμη. Αυτά χρησιμοποιούνται για να πιστοποιήσουν τον χρήστη και την φορητή μνήμη ως προς την συσκευή.

Κάθε φορά που ο χρήστης επιθυμεί να αυθεντικοποιηθεί στην συσκευή θα πρέπει να συνδέσει την φορητή μνήμη και να δώσει τα κατάλληλα συνθηματικά. Στην συνέχεια και όταν η συσκευή χρειαστεί να αυθεντικοποιηθεί σε κάποιο δίκτυο και ενώ γνωρίζει το ένα μέρος από τα συνθηματικά θα πρέπει να αναζητήσει στην φορητή μνήμη το άλλο μέρος. Αυτό βρίσκεται σε σημείο που είναι προκαθορισμένο και γνωρίζει η συσκευή.

Εκτελώντας στην συνέχεια κατάλληλες πράξεις μέσω του λογισμικού που διαθέτει κάνει την επανασύνδεση αυτών. Με τον τρόπο αυτό θα καταλήξει στο πιστοποιητικό μέσω του οποίου θα αυθεντικοποιηθεί στο δίκτυο. Θα πρέπει να επισημανθεί ότι τα πιστοποιητικά αυτά μπορεί να προέρχονται από κάποια αρχή πιστοποίησης που τα εκδίδει βάσει των ιδιοτήτων του χρήστη και τα φυσικά χαρακτηριστικά της συσκευής ή σπανιότερα προέρχονται αποκλειστικά από την αρχιτεκτονική του συστήματος ή άλλες παραμέτρους.

ΚΕΦΑΛΑΙΟ 10^{Ο}

Συμπεράσματα

Σύμφωνα με την αρχιτεκτονική του δικτύου, ένα δίκτυο μπορεί να έχει υποδομή (σταθερά σημεία πρόσβασης) ή να μην έχει υποδομή (adhoc και δίκτυα αισθητήρων). Η διασφάλιση της αξιόπιστης και της ασφαλής δρομολόγησης καθώς και η διατήρηση ενός επιπέδου εμπιστοσύνης μεταξύ των κόμβων του δικτύου είναι απαραίτητη για τη συνέχιση της παροχής υπηρεσιών μέσω αυτών των δικτύων.

Από την πλευρά του τερματικού σταθμού δηλαδή των κόμβων, είναι σημαντικό να προστατεύσουμε τους πόρους του (μπαταρία, δίσκος, CPU) κατά της κατάχρησης και να διασφαλιστεί το απόρρητο των δεδομένων του. Σε ένα adhoc δίκτυο καθίσταται απαραίτητο να διασφαλιστεί η ακεραιότητα του τερματικού σταθμού δεδομένου ότι διαδραματίζει έναν διπλό ρόλο, αυτού του δρομολογητή (router) και του τερματικού σταθμού.

Η δυσκολία του σχεδιασμού λύσεων ασφαλείας δεν προέρχεται μόνο από τη διασφάλιση της σταθερής αντιμετώπισης των πιθανών επιθέσεων ή από την εξασφάλιση ότι δεν θα επιβραδυνθούν οι επικοινωνίες αλλά πρέπει να βελτιστοποιηθεί η χρήση των πόρων σε εύρος ζώνης, μνήμης, μπαταρίας, κλπ . Ακόμη πιο σημαντικό σε αυτό το ανοικτό πλαίσιο του ασύρματου δικτύου είναι να εξασφαλίζεται η ανωνυμία και η προστασία της ιδιωτικής ζωής επιτρέποντας ταυτόχρονα την ιχνηλασιμότητα για νομικούς λόγους δηλαδή την πληρότητα των πληροφοριών σε κάθε βήμα μιας αλυσίδας διεργασιών παρέχοντας έτσι την δυνατότητα για τον χρονικό συσχετισμό-επαλήθευση των πληροφοριών.

Επίσης πρέπει τα συστήματα να σχεδιάζονται με μοντέλα εμπιστοσύνης τα οποία θα πρέπει να προσφέρουν υψηλό επίπεδο εμπιστοσύνης έναντι των κλασικών μηχανισμών ασφαλείας και έτσι τα μελλοντικά δίκτυα θα πρέπει να εφαρμόζουν και τα δύο μοντέλα δηλαδή της ασφάλειας και της εμπιστοσύνης.

Οι μηχανισμοί ασφαλείας που παρουσιάστηκαν παραπάνω είναι μια πρακτική απάντηση σε συγκεκριμένα προβλήματα που ανακύπτουν στα επίπεδα του προτύπου OSI. Ωστόσο, οι λύσεις που προτείνονται καλύπτουν μόνο ένα υποσύνολο όλων των πιθανών απειλών και είναι δύσκολο να ενσωματωθούν μεταξύ τους. Μια πλήρης υποδομή ασφαλείας πρέπει να εξετάσει ένα ευρύ φάσμα επιθέσεων και έτσι πρέπει να ενσωματώνει πολλά στοιχεία. Επιπλέον, οι ανάγκες ασφάλειας μπορεί να ποικίλλουν ανάλογα με τα διάφορα σενάρια δικτύωσης και τους μηχανισμούς ασφάλειας οι οποίοι εγκρίθηκαν για την καταπολέμηση της εσφαλμένης συμπεριφοράς ή την διαταραχή των κόμβων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Marlon McBride, Mustafa Masacioglu, Control Based Mobile Ad Hoc Networking For Survivable - Dynamic -Mobile Special Operation Force Communications, Naval Postgraduate School, Monterey California, September 2009
[2] Anil Kumar Verma, Design And Development Of A Routing Protocol For Mobile Ad Hoc Networks (MANETs), Thapar University, Patalia, Arpil 2007
[3] Deshpande Vivek S, Security in Ad-Hoc Routing Protocols, Maharashtra Institute Of Technology Women Engineering, India
[4] Erdal Çayırcı (NATO Joint Warfare Centre) , Chunming Rong (University of Stavanger),Security in Wireless Ad Hoc and Sensor Networks (Book), Norway, 2009
[5] Al-Sakil Kham Pathan, Security Of Self Organizing Networks (Manet Wsn WMN Vanet), USA, 2011
[6] Vesa Kärpijoki, Security in Ad Hoc Networks, Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology , Finland
[7] Adam Burg, Ad hoc Network Specific Attacks, Technological University of Munich, 2003
[8] A.Economides, A. Pomportsis, Gkarafli Stamati, Networking Technologies– MANET, University Of Macedonia, 2005
[9] Theologou Mixahl, Koutsoubelas Dimitrios, Kwstoydhs Hlias, Security in ad hoc networks and sensor networks, National Technical University Of Athens, 2008
[10] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, A Survey Of Attacks And Countermeasures in Mobile Ad Hoc Networks, Department of Computer Science and Engineering, Florida Atlantic University
[11] Kamanshis Biswas, Md. Liakat Ali, Security Threats in Mobile Ad Hoc Network , Department of Interaction and System Design, School of Engineering Blekinge Institute of Technology , Sweden, 2007
[12] Yibghua Guo, Detecting Manets Against Flooding Attacks By Detective Measures, Institute for telecommunication Research, University Of South Australia, 2008
[13] C.Prasanna lakshmi & K.Yasasvi, Secure Routing Protocols for Wireless AdHoc Networks, Sri Venkatesa Perumal College of Engineering and Technology, 2010 (http://www.yuvaengineers.com/?p=699)
[14] H Yang H Y. Luo, F Ye S W. Lu L Zhang, Security in Mobile Ad hoc Networks: Challenges and solutions, University of California, 2004
[15] Rutvij H. Jhaveri1, Ashish D. Patel2, Jatin D. Parmar3 ,Bhavin I. Shah4, MANET Routing Protocols and Wormhole Attack against AODV, Department of Computer Engineering and Information Technology, S.V.M. Institute of Technology, Bharuch, India
[16] Dimitris Glynos, Panayiotis Kotzanikolaou, Christos Douligeris, Preventing Impersonation Attacks in MANET with Multi-factor Authentication, Department of Informatics, University of Piraeus

ΠΑΡΑΡΤΗΜΑ

- **WLAN (Wireless Local Area Network):** Είναι ασύρματο τοπικό δίκτυο μεταξύ δύο ή περισσότερων computer χωρίς τη χρήση καλωδίων.
- **WPAN (Wireless Personal Area Network):** Είναι ασύρματο τοπικό δίκτυο μεταξύ υπολογιστών για επικοινωνία μεταξύ συσκευών όπως το τηλέφωνο και το PDA, κοντά σε ένα άτομο.
- **WMAN (Wireless Metropolitan Area Network):** Είναι ασύρματο δίκτυο για μία πόλη.
- **WWAN (Wireless Wide Area Network):** Είναι ασύρματο δίκτυο όπου οι υπολογιστές είναι πολύ μακριά ο ένας από τον άλλο.
- **GSM (Global System for Mobile communication):** Είναι ψηφιακό σύστημα κινητής τηλεφωνίας που χρησιμοποιείται ευρέως στην Ευρώπη και σε άλλα μέρη του κόσμου.
- **Symmetric encryption:** Είναι η μετάφραση των δεδομένων σε έναν μυστικό κωδικό. Πρόκειται για κρυπτογράφηση όπου χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση του μηνύματος.
- **Assymetric encryption:** Πρόκειται για κρυπτογράφηση που χρησιμοποιεί διαφορετικό κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση του μηνύματος.
- **OSI (Open Systems Interconnection):** Είναι μια διαστρωματωμένη, αφηρημένη περιγραφή για σχεδίαση επικοινωνιών και δικτυακών πρωτοκόλλων για υπολογιστές. Είναι γνωστό και ως Μοντέλο των επτά επιπέδων.
- **MAC (Medium Access Control):** Υποεπίπεδο ελέγχου προσπέλασης μέσου του επιπέδου ζεύξης δεδομένων του OSI μοντέλου
- **IP address:** Είναι η ταυτότητα ενός υπολογιστή ή μιας συσκευής σε ένα TCP/IP δίκτυο.
- **BSS (Basic Service Set):** Είναι εργαλείο για την αρχιτεκτονική IEEE 802.11 WLAN.

-